PLANEACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL ÁREA DE SISTEMAS DE UNA EMPRESA FABRICANTE DE PRODUCTOS ELECTRÓNICOS BAJO LA NORMA ISO 27001:2013

KATHERINE FERNANDA BULLA VALENCIA
NATALIA IVONNE FORERO LOZANO

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA
ESPECIALIZACIÓN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2016

PLANEACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL ÁREA DE SISTEMAS DE UNA EMPRESA FABRICANTE DE PRODUCTOS ELECTRÓNICOS BAJO LA NORMA ISO 27001:2013

KATHERINE FERNANDA BULLA VALENCIA
NATALIA IVONNE FORERO LOZANO

Trabajo de grado para optar al título de
Especialista en Seguridad de la información

Director: ÁLVARO ESCOBAR ESCOBAR
Ingeniero de Sistemas

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA
ESPECIALIZACIÓN SEGURIDAD INFORMÁTICA
Bogotá D.C.
2016

Nota de Aceptación:

_____
_____
_____

_____
Firma del Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Bogotá, Febrero de 2016

DEDICATORIA

Primero que todo le damos gracias a Dios quien nos ayudó y nos guío por el buen camino, dándonos fuerzas para salir adelante y no rendirnos en cada uno de los problemas que se nos presentaban, enseñándonos a encarar las adversidades sin perder nunca la dignidad, ni desfallecer en el intento

A nuestras familias, quienes con sus consejos, apoyo, amor, ayuda en los momentos más difíciles nos ayudaron a culminar esta etapa tan importante para nuestras vidas.

AGRADECIMIENTOS

Las autoras expresan sus agradecimientos a:

Álvaro Escobar Escobar, director del proyecto

A la Universidad Piloto de Colombia

A todas aquellas personas que de una u otra forma colaboraron en la elaboración de este proyecto.

CONTENIDO

Pág.

INTRODUCCIÓN 14

1. JUSTIFICACIÓN 16

2. OBJETIVOS 17

2.1 OBJETIVO GENERAL 17

2.2 OBJETIVOS ESPECÍFICOS 17

3. MARCO TEÓRICO 18

3.1 ORIGEN DE LA SEGURIDAD 18

3.2 POLÍTICAS DE SEGURIDAD 19

3.2.1 Responsables. 19

3.3 NORMA ISO 27001:2013 20

3.3.1 Confiabilidad de los datos. 20

3.3.2 Disponibilidad de los datos. 20

3.4 ¿POR QUÉ ES NECESARIA LA SEGURIDAD DE LA INFORMACIÓN EN? 20

3.5 CICLO PHVA (planificar, hacer, verificar y actuar) 21

3.5.1 Planificar 21

3.5.2 Hacer 21

3.5.3 Verificar 21

3.5.4 Actuar 21

4. METODOLOGÍA 22

4.1 DISEÑO 22

4.2 PARTICIPANTES 22

4.3 INSTRUMENTOS 22

5. INFORMACIÓN EMPRESARIAL 26

5.1 RESEÑA HISTÓRICA 26

5.2 MISIÓN - VISIÓN 26

5.3 UBICACIÓN GEOGRÁFICA 26

5.4 ESTRUCTURA ORGANIZACIONAL 26

6. ESTADO ACTUAL ACTIVOS DE 28

6.1 ACTIVOS DE HARDWARE 28

6.2 ACTIVOS DE SOFTWARE 29

6.3 ACTIVOS LÓGICOS 29

7. APLICACIÓN ENCUESTA DIAGNÓSTICO 30

7.1 RESULTADOS ENCUESTA REALIZADA 30

7.2 ENCUESTA REALIZADA A USUARIOS 31

7.2.1 ¿Cree usted que posee información de vital importancia para la empresa? 31
7.2.2 ¿Cree usted que existen riesgos para este tipo de información (Pérdida, daños, etc.)? 32
7.2.3 ¿Conoce las implicaciones que acarrean una posible pérdida de información o una falla en los sistemas tecnológicos de la empresa? 33
7.2.4 ¿Realiza copias de seguridad o algún plan de contingencia en caso de fallos en la información o en los sistemas de información? 34
7.2.5 ¿Conoce usted de cuántos ordenadores dispone su empresa? 35
7.2.6 Los ordenadores de su empresa, ¿tienen instalado antivirus? 36
7.2.7 ¿Se realiza un mantenimiento informático periódico sobre los ordenadores de la empresa? 37
7.2.8 ¿Disponen de servidor central de datos en su empresa? 38
7.2.9 Sobre dicho servidor, ¿Se realiza un mantenimiento informático periódico? 39
7.2.10 ¿Dispone de baterías (SAI), APC, plantas eléctricas o algún otro dispositivo para cada ordenador y servidor, para evitar apagones o sobretensiones? 40
7.2.11 ¿Conoce usted si la empresa tiene políticas de seguridad informática? 41
7.2.12 ¿Cuenta con un plan de contingencia en caso de un desastre natural o un mal manejo de información? 42
7.2.13 ¿Conoce usted de los riesgos informáticos a los que están expuestos? 43
7.2.14 ¿Siente que no está expuesto a los ataques informáticos y que su información está segura? 44
7.2.15 ¿Usted maneja dispositivos extraíbles como: memorias USB, CD, DVD, discos duros externos? 45

7.2.16 ¿Antes de ingresar los dispositivos externos, los reporta al área de sistemas? 46
7.2.17 ¿La empresa permite el acceso a internet y redes sociales? 47
7.2.18 ¿Cómo manejan el ingreso al sistema informático de la empresa, por medio de usuario y claves o dispositivos electrónicos? 48
7.2.19 ¿El acceso a los recursos de red es restringido o no? 49
7.2.20 ¿La empresa cuenta con redes Wi-Fi? 50
7.2.21 ¿Realiza descargas de archivos desde internet (Música, videos, imágenes, etc.)? 51

8. VERIFICACIÓN Y APLICACIÓN DE LA NORMA ISO 27001:2013 52
8.1 MATRIZ DE RIESGOS Y ACCIONES MITIGANTES 52
8.1.1 Valoración del riesgo 52
8.1.2 Matriz de riesgos 53
8.2 RESULTADO DE INCUMPLIMIENTO DE LA NORMA ISO 27001 84

9. VERIFICACIÓN Y APLICACIÓN DE LA NORMA ISO 27001:2013 87
9.1 HALLAZGO 01 POLÍTICA PARA LA SEGURIDAD DE LA INFORMACIÓ 87
9.2 HALLAZGO 02 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN 88
9.3 HALLAZGO 03 SEGURIDAD DE LOS RECURSOS 89
9.4 HALLAZGO 04 GESTIÓN DE ACTIVOS 90
9.5 HALLAZGO 05 CONTROL DE ACCESO 91

9.6 HALLAZGO 06 CRIPTOGRAFÍA 92

9.7 HALLAZGO 07 SEGURIDAD FÍSICA Y AMBIENTAL 93

9.8 HALLAZGO 08 SEGURIDAD DE LAS OPERACIONES 95

9.9 HALLAZGO 09 SEGURIDAD DE LAS COMUNICACIONES 96

9.10 HALLAZGO 10 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS 97

9.11 HALLAZGO 11 RELACIONES CON LOS PROVEEDORES 98

9.12 HALLAZGO 12 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN 100

9.13 HALLAZGO 03 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIO 101

9.14 HALLAZGO 14 CUMPLIMIENTO 102

10. CONCLUSIONES 105

11. RECOMENDACIONES 107

BIBLIOGRAFÍA 113

ANEXOS

LISTA DE FIGURAS

Pág.

Figura 1. Estructura organizacional 27

Figura 2. Resultado estadístico pregunta No. 1 31

Figura 3. Resultado estadístico pregunta No. 2 32

Figura 4. Resultado estadístico pregunta No. 3 33

Figura 5. Resultado estadístico pregunta No. 4 34

Figura 6. Resultado estadístico pregunta No. 5 35

Figura 7. Resultado estadístico pregunta No. 6 36

Figura 8. Resultado estadístico pregunta No. 7 37

Figura 9. Resultado estadístico pregunta No. 8 38

Figura 10. Resultado estadístico pregunta No. 9 39

Figura 11. Resultados estadístico pregunta No. 10 40

Figura 12. Resultado estadístico pregunta No. 11 41

Figura 13. Resultado estadístico pregunta No.12 42

Figura 14. Resultados estadístico pregunta No.13 43

Figura 15. Resultados estadístico pregunta No. 14 44

Figura 16. Resultados estadístico pregunta No. 15 45

Figura 17. Resultados estadístico pregunta No. 16 46

Figura 18. Resultados estadístico pregunta No. 17 47

Figura 19. Resultados estadístico pregunta No. 18 48

Figura 20. Resultados estadístico pregunta No. 19 49

Figura 21. Resultados estadístico pregunta No. 20 50

Figura 22. Resultados estadístico pregunta No. 21 51

Figura 23. Incumplimiento Objetivos de control 83

Figura 28. Porcentaje de incumplimiento 85

Figura 29. Indicadores de cumplimiento 86

LISTA DE CUADROS

Pág.

Cuadro 1 Consolidado encuesta diagnóstico de seguridad informática 23

Cuadro 2 Descripción de activos de hardware 28

Cuadro 3 Descripción de activos software 29

Cuadro 4 Descripción de activos lógicos 29

Cuadro 5 Valores de riesgo 52

Cuadro 6 Matriz de riesgo 54

INTRODUCCIÓN

Este proyecto de grado pretende diagnosticar la situación actual de la seguridad de la información en la empresa de fabricación de productos electrodomésticos específicamente para el área de sistemas, inicialmente el desarrollo de este documento nace del interés de la entidad en conocer su nivel de protección en cuanto a este tema. El alcance de este diagnóstico de seguridad de la información está orientado para la Jefatura de Sistemas, que posee la mayoría de la información requerida para culminar con éxito este proyecto.

Tiene como principal actividad comercial la fabricación de aparatos de distribución y control de la energía electrónica; elabora, diseña, produce, y comercializa artículos electrónicos los cuales se encuentran clasificados en quince líneas, por nombrar alguna de ellas, están: la línea Doumo (maneja interruptores, pulsadores, tomacorrientes, etc.), la línea Cooper Lighting (luminarias de emergencia), línea de Tableros y Cajas Monofásicas.

Esta entidad garantiza calidad en los productos que fábrica, realizando diferentes controles de verificación, seguimiento, inspección y ensayo desde la recepción de materias primas, proceso productivo y ensayos finales del producto terminado, basándose en los requisitos exigidos por las normas del sector eléctrico ya sea de carácter internacional como son IEC (Internacional Electrotechnical Comisión), NTC (Norma Técnicas Colombianas), RETIE (Reglamento Técnico de Instalaciones Eléctricas) Normas Técnicas Nom México. Adicional a estas normas, está certificada en cuanto al producto por CIDET, ICONTEC y ANCE con auditorías periódicas y eventualmente a través de equivalencias expedidas por el Ministerio de Minas y Energía y controladas por la Superintendencia de Industria y Comercio.

El dinamismo en la construcción de obras civiles, las nuevas facilidades de financiación para la utilización de maquinaria y el aumento de inversión privada en el sector, permitieron que la actividad creciera el doble del ritmo de la tasa de inflación, con unos retornos aún más importantes. De acuerdo a un análisis que realizó la página web “La Nota Economica.co” información que reposa en el Vademécum Empresarial 2009/2010 para Medianos Sectores en la Subcategoría Maquinaria y Equipo, esta empresa se posiciona en el mercado con el puesto 107 de 403 empresas en Colombia.

Con el fin dar un realce un poco más real y de llegar a considerar la importancia y la relevancia que tiene este tema se tuvo en cuenta una encuesta emitida por la ISO (International Systems Organization) 2013 evaluada en todo el mundo para el caso específico de este proyecto, se tomó el resultado por sectores empresariales para el año 2013, e indica que para el sector de maquinaria y equipo en la cual se encuentra ubicada la empresa el porcentaje de participación de las empresas

iguales o similares a lo que indica que este tipo de organizaciones no han contemplado en ningún momento de su vida empresarial la protección de escenarios que involucren la información como parte de las preocupaciones internas.

El resultado de la encuesta, permite exaltar y motivar aún más este proyecto, toda vez, que el cambio de mentalidad y el deseo por mejorar sus procesos, considerando la seguridad de la información como parte de estos objetivos es de gran satisfacción. De igual manera la elaboración de un diagnóstico apropiado y coherente, posiblemente contribuya en impulsar a ser la primera empresa del sector que se encuentre certificada bajo la norma ISO 27001:2013.

Este proyecto evalúa la situación real, basándose en la norma ISO 27001:2013 con el fin de establecer claramente cuáles son las falencias que hacen que se incumpla y cuáles serían las posibles recomendaciones que podrá dar inicio para la implementación de la norma, lo que permitirá ser más competitivos en el mercado. Siendo esto, un valor agregado a la actividad principal que desarrollan. Así mismo, la generación de una cultura al interior de la empresa, junto con sus empleados consistentes en el manejo adecuado de la información, como un activo más de la organización.

1. JUSTIFICACIÓN

En décadas pasadas el poder de los individuos se manifestaba mediante el control de los recursos tangibles, en el mundo globalizado de hoy el poder está dado por el conocimiento, un recurso eminentemente intangible. En respuesta a esto, las nuevas tecnologías aportan una herramienta fundamental para el manejo de la información, como pilar del conocimiento. Es así que en los últimos años el crecimiento de la tecnología a nivel mundial, ha generado una necesidad constante de satisfacer al usuario final en cuanto al flujo de información, trayendo consigo un centenar de riesgos informáticos una vez que se ingresa al ciberespacio, en donde los usuarios y su información son potencialmente vulnerables; razón por la cual el tema de Seguridad de la Información viene tomando fuerza e importancia; tanto para los usuarios en general como al interior de las organizaciones públicas y privadas.

Como primera medida para brindar seguridad a la información, es indispensable conocer en profundidad los procesos asociados a la misma, así como los individuos responsables de su manejo. En este sentido la seguridad de la información debe partir de un diagnóstico detallado que describa a fondo el estado actual del flujo de información y todas las variables relacionadas en el entorno en el que se emplea cualquier tipo de información particular o especializada de carácter reservada.

Por lo tanto, un buen diagnóstico debe proveer información útil para la creación y puesta en marcha de protocolos de seguridad que permitan mejorar los mecanismos existentes o provean nuevos mecanismos que respondan a las necesidades, con miras no sólo a la protección de la información como tal, sino a la prevención de futuros incidentes; basándose tanto en la experiencia del usuario como en la versatilidad y profesionalismo de quien realice el diagnóstico.

En este contexto la entidad que es pionera en la comercialización, producción, manejo y distribución de artículos electrónicos; tiene en la seguridad de la información una necesidad imperiosa por mejorar sus procesos y ofrecer a sus clientes un mejor servicio. Pese a esto no existe evidencia que permita establecer que la empresa cuenta con mecanismos de seguridad de la información suficientemente robustos, en coherencia con la corresponsabilidad que ésta tiene en cuanto a su ámbito comercial y su alta imagen empresarial que ha propendido por mantener desde su creación.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Planeación de un sistema de gestión de seguridad de la información para el área de sistemas de una empresa fabricante de productos electrónicos bajo la norma ISO 27001:2013

2.2 OBJETIVOS ESPECÍFICOS

Levantar la información necesaria para la planificación de un sistema de gestión de seguridad de la información para el área de sistemas basada en la norma ISO 27001:2013

Consolidar la información encontrada para la planificación de un sistema de gestión de seguridad de la información para el área de sistemas basada en la norma ISO 27001:2013.

Identificar, valorar y gestionar la información obtenida para la realización del diagnóstico

Elaborar un análisis de riesgo para la empresa basado en la aplicación de la norma ISO 27001:2013

Aplicar y analizar las encuestas realizadas al área de sistemas y demás funcionarios de la empresa con el fin de acoplar toda la información encontrada para la realización de hallazgos.

Valorar cada uno de los hallazgos encontrados, con sus causas, efecto, conclusiones y recomendaciones.

3. MARCO TEÓRICO

Con el fin de contextualizar el tema de seguridad de la información y la importancia de la misma y considerando el riesgo latente que existe en las entidades privadas en Colombia, se indica a continuación algunas definiciones y conceptos básicos que se deben contemplar para la realización de la propuesta:

3.1 ORIGEN DE LA SEGURIDAD

Considerando que el ser humano desde sus orígenes ha buscado protección en todos los aspectos, como por ejemplo seguridad para la familia, seguridad en sus bienes, seguridad personal, etc., se puede considerar que este tema viene de tiempo atrás, este pensamiento fue estudiado por James P. Anderson autor del libro “Computer Security Threat Monitoring and Surveillance”, el cual realizó un análisis y estableció que la seguridad nace propiamente del sentir del ser humano y ha logrado que evolucione el concepto con las necesidades propias de las personas.

También con la evolución del hombre y sus necesidades por mejorar su calidad de vida, llegan con este proceso los sistemas informáticos que buscaron agilizar su trabajo y contener toda la información considerada para la sociedad simples datos compuestos bits y byte. Comenzó la era de los computadores y con ellos el requerimiento de conectarlos entre sí, con un propósito fundamental de enviar y recibir información; desde cualquier lugar del mundo; pero con esta necesidad llego también el asegurar la información que se estaba transfiriendo. Es por esto, que se puede concluir que el hombre y los sistemas tienen un tema en un común “Protección”.[1]

Para las organizaciones y las personas en Colombia, el concepto de la seguridad de la información nace desde el momento en que se genera una necesidad de salvaguardar y proteger lo que es considerado vital y/o prioridad; todo esto se evidencia en el diario vivir y la celeridad en el que se encuentra el mundo; estas acciones se reflejan en la urgencia por establecer protección a los procesos que coadyuvar a evitar en gran medida los riesgos que traen inherentes a ellos.

La seguridad de la información brinda desde diferentes mecanismos la identificación de amenazas y vulnerabilidades que afectan los sistemas y que generan en muchos casos daños irreparables, ocasionados por personas que poseen conocimientos en sistemas informáticos para causar daños; de esta manera se involucra a este tema:

[1] ANDERSON, James P. Computer Security Threat Monitoring and Surveillance. 1998. [en línea], consultado el 2 de septiembre de 2015]. Disponible en: https://www.sans.org/.../history-evolution-intrusion.

Los hackers, para definir que es, el diccionario Merrian-Webster establece una definición “una persona que secretamente tiene acceso a un sistema informático con el fin de obtener información, causa daños, etc.: una persona que interviene negativamente en un sistema informático”.

3.2 POLÍTICAS DE SEGURIDAD

Teniendo en cuenta que la busca conocer el estado actual de su seguridad mediante un diagnóstico de seguridad de la información; y un punto importante para dar inicio a la implementación de un sistema de seguridad, son las políticas de seguridad. Estas políticas de seguridad no son netamente un mecanismo de sanción, es un concepto de saber que se quiere proteger y cómo hacerlo. Contemplar una política y que haya éxito, corresponde hacer parte a todo el personal de la entidad y de reconocer la información como activo. Por tal razón se deben establecer unos requisitos que se deben establecer para el personal que intervienen directa e indirectamente a los sistemas de información y deben ser de tipo:

- Prohibitiva, es decir, todo lo que no está expresamente permitido está denegado.

- Permisiva, es decir, todo lo que no está expresamente prohibido está permitido[2].

3.2.1 Responsables. La política de seguridad contempla la necesidad de delegar responsabilidades; es decir, personal encargado de hacer que estas políticas sean cumplidas por la empresa. Se cuenta con un ingeniero de sistemas para toda la planta, es por esto que esta persona debe contar con apoyo para que estas políticas se lleven a cabo se debe contar con otra persona que se encuentre ligada a la norma ISO 27001:2013 que apoye las políticas de seguridad en la compañía. Se debe contar con un responsable en seguridad informática que cumpla las funciones de supervisión, cumplimiento, mantenimiento, actualizaciones, capacitaciones e informes periódicamente a gerencia.

Para la realización de estas políticas se deben tener en cuenta la normatividad que coadyuvan a la empresa a poseer una mejor gestión de seguridad informática.

[2] PTOLOMEO.UNAM.MX. Definiciones e historia de la seguridad informática capitulo1, [en línea] [consultado el 2 de septiembre de 2015]. Disponible en: http://www.ptolomeo.unam. mx:8080/ xmlui/bitstream/handle/132.248.52.100/217/A4.pdf?sequence=4 Octubre de 2005, p. 7-8.

3.3 NORMA ISO 27001:2013

Es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. Además esta norma establece 114 controles que permiten a la organización cumplir con los requisitos de seguridad de la propia organización estableciendo los 3 principios fundamentales en los que se basa la seguridad informática que son:

3.3.1 Confiabilidad de los datos. Se refiere a la capacidad del sistema para evitar que personas o procesos no autorizados puedan acceder a la información almacenada en él[3].

3.3.2 Disponibilidad de los datos. Se refiere a él funcionamiento eficientemente y que es capaz de recuperarse rápidamente en caso de falla. Es decir que la información se pueda utilizar cuando se requiera[4].

3.3.3 Integridad de los datos. El sistema no debe modificar ni corromper la información que almacena, o permitir que alguien no autorizado lo haga. Permitiendo asegurar que no ha sido falsificada la información[5]. Teniendo en cuenta que este tipo de norma puede ser implementada en cualquier tipo de organización ya sea grande, pequeña, privada o pública. Es por este motivo es seleccionada la empresa para la realización de una propuesta de gestión y seguridad basado en la norma ISO 27001:2013

3.4 ¿POR QUÉ ES NECESARIA LA SEGURIDAD DE LA INFORMACIÓN?

Es necesaria la seguridad de la información, toda vez que esta empresa actualmente no cuenta con políticas de seguridad que brinden protección a los sistemas de información. La inexistencia de las políticas constantemente está expuesta a fraudes, daños y/o ataques.

Esto puede conllevar a causar varios daños en cuanto a su competitividad, rentabilidad, el cumplimiento legal y la imagen empresarial.

[3] HEINEKEN TEAM. Seguridad y protección de la información: Introducción a la problemática de la seguridad informática. [en línea]. [consultado el 2 de septiembre de 2015]. Disponible en: http://www0.unsl.edu.ar/~tecno/redes%202008/seguridadinformatica.pdf agosto 2001, p.2.

3.5 CICLO PHVA (planificar, hacer, verificar y actuar)

Este modelo es utilizado para realizar la implementación de un sistema de gestión de seguridad informática dado que permite realizar las actividades que marquen un orden lógico, organizado y que permita poder lograr un buen diagnóstico.

3.5.1 Planificar

- Definir políticas de seguridad.
- Determinar el alcance.
- Valorar activos.
- Analizar el riesgo.
- Gestionar el riesgo.
- Aplicar controles de la norma ISO 27001:2013

3.5.2 Hacer

- Implementar plan de gestión de riesgos Código de práctica para la gestión de la seguridad de la información.
- Implementar controles.

3.5.3 Verificar

- Verificación de implementación de gestión de riesgo.
- Revisión de procesos de monitoreo.
- Revisión de niveles de riesgo.
- Revisión de auditorías internas.

3.5.4 Actuar

- Implementaciones de mejoras.
- Adoptar medidas preventivas y correctivas.
- Comunicación de resultados.

4. METODOLOGÍA

4.1 DISEÑO

Se realizó un diagnóstico, bajo el concepto completamente académico, que permitió evidenciar los riesgos, aplicando dos instrumentos para verificar la información (encuestas) al área de sistemas y (cuestionarios) para los usuarios que acceden al sistema.

Así mismo, se utilizó una matriz de riesgo para el proceso en estudio (Jefatura de Sistemas) que permitió organizar cada uno de los dominios, objetivos de control, riesgos y controles establecidos en el Anexo A de la norma ISO 27001:2013, de tal manera que el resultado de este instrumento permita mitigar los riesgos más importantes como también obtener una visión más clara de la situación real de esta área.

Los datos que hicieron parte de esta matriz, fueron considerados como información de alta confiabilidad, dado que se extrajeron directamente por parte del Jefe de la Jefatura de Sistemas y por el personal que hace parte de la empresa

4.2 PARTICIPANTES

Las personas que participaron en esta propuesta son una muestra de los empleados y usuarios que manipulan y/o accede de los sistemas de información que maneja la entidad. Los empleados que participaron son profesionales, directamente encargados de los sistemas de información y seguridad. Por su parte los usuarios, fueron personas vinculadas a la empresa que utilizan los recursos informáticos, más no directamente relacionados con el área de seguridad.

La entidad cuenta con una persona vinculada al área de seguridad, que participó en el estudio. Así mismo, se consideraron cuarenta (40) usuarios de los sistemas de información, de los cuales se seleccionó una muestra aleatoria representativa equivalente al 75% de la población.

4.3 INSTRUMENTOS

Se diseñó una encuesta (para aplicación virtual o en papel) de 133 ítems (preguntas cerradas, para que el personal vinculado al área de seguridad que evalué el sistema, bajo unos estándares previamente establecidos **(Ver anexo 1).** De igual forma, se creó un breve cuestionario con 21 ítems (preguntas abiertas), para que los usuarios seleccionados evalúen el sistema de seguridad, los

resultados fueron consolidados en el (Cuadro No 1. Consolidado encuesta diagnóstico de seguridad informática).

Cuadro No 1. Consolidado encuesta diagnóstico de seguridad informática.

Consolidado encuesta diagnóstico de seguridad informática para Ave Colombiana S.A.S.

Número de encuestas	¿Cree usted que posee información de vital importancia para la empresa?	¿Cree usted que existen riesgos para este tipo de información. (perdida, daños, etc)?	¿Conoce las implicaciones que acarrea una posible pérdida de información o un fallo en los sistemas tecnológicos de la empres	¿Realiza copias de seguridad o algún plan de contingencia en caso de fallos en la información o en los sistemas (	¿conoce usted de cuántos ordenadores dispone su empresa?	¿Los ordenadores de su empresa, ¿tienen instalado antivirus?	¿Se realiza un mantenimiento informático periódico sobre los ordenadores de la empres	¿Disponen de servidor central de datos en su empresa?	¿Sobre dicho servidor, ¿se realiza un mantenimiento informático periódic
1	1	2	1	1	1	1	2	2	2
2	1	1	2	1	1	1	2	1	2
3	1	2	2	1	1	1	2	1	2
4	1	2	2	1	2	1	2	1	2
5	1	2	2	1	2	1	2	2	2
6	1	1	2	1	2	1	2	1	2
7	2	1	2	1	2	1	2	1	2
8	2	2	2	1	2	1	2	1	2
9	2	2	2	1	2	1	2	2	2
10	2	2	2	1	2	1	2	2	2
11	2	1	2	1	2	1	2	2	2
12	1	2	2	1	2	1	2	2	2
13	1	2	2	1	2	1	2	1	2
14	1	1	2	1	2	1	2	1	2
15	2	2	2	1	2	1	2	1	2
16	2	1	2	1	2	1	2	2	2
17	2	2	2	1	2	1	2	2	2
18	2	2	2	1	2	1	2	2	2
19	2	2	1	1	2	1	2	1	2
20	2	1	2	1	2	1	2	1	2
21	2	2	2	1	2	1	2	2	2
22	2	1	2	1	2	1	2	2	2
23	2	2	2	1	2	1	2	1	2
24	2	1	2	1	2	1	2	1	2
25	2	1	2	1	2	1	2	2	2
26	2	1	2	1	2	1	2	2	2
27	2	2	2	1	2	1	2	2	2
28	2	2	2	1	2	1	2	2	2
29	2	2	2	1	2	1	2	1	2
30	2	2	1	1	2	1	2	2	2
31	2	2	1	1	2	1	2	1	2

Cuadro 1.continuación

Consolidado encuesta diagnóstico de seguridad informática para Ave Colombiana S.A.S.

¿Dispone de baterías (SAI), APC, plantas eléctricas o algún otro dispositivo para cada ordenador y servidor, para evitar apagor	¿Conoce usted si la empresa tiene políticas de seguridad informática?	¿Cuenta con un plan de contingencia en caso de un desastre natural o un mal manejo de información?	¿Conoce usted de los riesgos informáticos a los que están expuestos?	¿Siente que no está expuesto a los ataques informáticos y que su información está segura?	¿Usted maneja dispositivos extraíbles como: memorias usb,cd, dvd, discos duros externos	¿Antes de ingresar los dispositivos externos, los reporta al área de sistemas? (Responda únicamente si la anterior respuesta	¿La empresa permite el acceso a internet y redes sociales?	¿Como manejan el ingreso al sistema informático de la empresa, por medio de usuario y claves o dispositivo	¿El acceso a los recursos de red es restringido o no?	¿La empresa cuenta con redes Wifi?	¿Realiza descargas de archivos desde internet (Música, videos, imágenes, etc)?
1	2	2	2	2	2	2	1	2	1	1	2
1	2	2	1	2	1	2	1	2	1	1	1
1	2	2	1	2	1	2	1	2	1	1	1
1	2	2	1	2	1	2	1	2	1	1	1
1	2	1	1	2	1	2	1	2	1	1	1
1	2	1	2	2	1	2	1	2	1	1	2
1	2	1	2	2	1	2	1	2	1	1	2
1	2	2	2	2	1	2	1	2	1	1	2
1	2	2	2	2	1	2	1	2	1	1	2
2	2	2	2	2	1	2	1	2	1	1	1
2	2	1	1	1	1	2	1	2	1	1	1
2	2	1	1	2	1	2	1	2	1	1	1
2	2	2	1	1	1	2	2	2	1	1	2
2	2	2	1	2	1	2	2	2	1	1	2
1	2	2	2	1	1	2	2	2	1	1	1
1	2	1	1	2	1	2	2	2	1	1	2
1	2	1	2	1	1	2	1	2	1	1	1
1	2	1	1	2	1	2	1	2	1	1	2
1	2	1	2	1	1	2	1	2	2	1	1
1	2	2	1	2	1	2	2	2	2	1	2
1	2	2	2	1	1	2	2	2	1	1	1
1	2	2	1	2	1	2	2	2	1	1	2
2	2	2	2	1	1	2	1	2	1	1	1
1	2	1	1	2	1	2	1	2	1	1	1
2	2	2	1	1	1	2	1	2	1	1	2
2	2	1	1	2	1	2	2	2	2	1	2
1	2	2	1	1	1	2	2	2	2	1	2
1	2	1	2	2	1	2	1	2	2	1	2
1	2	1	2	1	1	2	1	2	1	1	1
2	2	2	2	2	1	2	2	2	1	1	1
2	2	1	2	2	1	2	2	2	1	1	1

Fuente: Autores

5. INFORMACIÓN EMPRESARIAL

5.1 RESEÑA HISTÓRICA

La empresa fue fundada hace 54 años, inicio labores comerciales como Ladrillera, luego con el transcurrir del tiempo tuvo la oportunidad de comenzar a incursionar en el ambiente de la importación de artículos electrónicos con la Empresa Ave Italiana. Fue esta entidad, quienes impulsaron para que se encuentre posicionada hoy en día como una de las mejores compañías que sobresalen por la terminación y calidad de productos electrónicos.

5.2 MISIÓN - VISIÓN

De acuerdo a las políticas de la Alta Gerencia, la Misión y la Visión fueron suspendidas por considerar que no se ajustaban a los lineamientos actuales de la entidad. Cuenta con una política, y objetivos ajustados directamente al producto.

5.3 UBICACIÓN GEOGRÁFICA

Se encuentra ubicada en el Municipio de Zipaquirá Km^3 Vía Nemocón.

5.4 ESTRUCTURA ORGANIZACIONAL

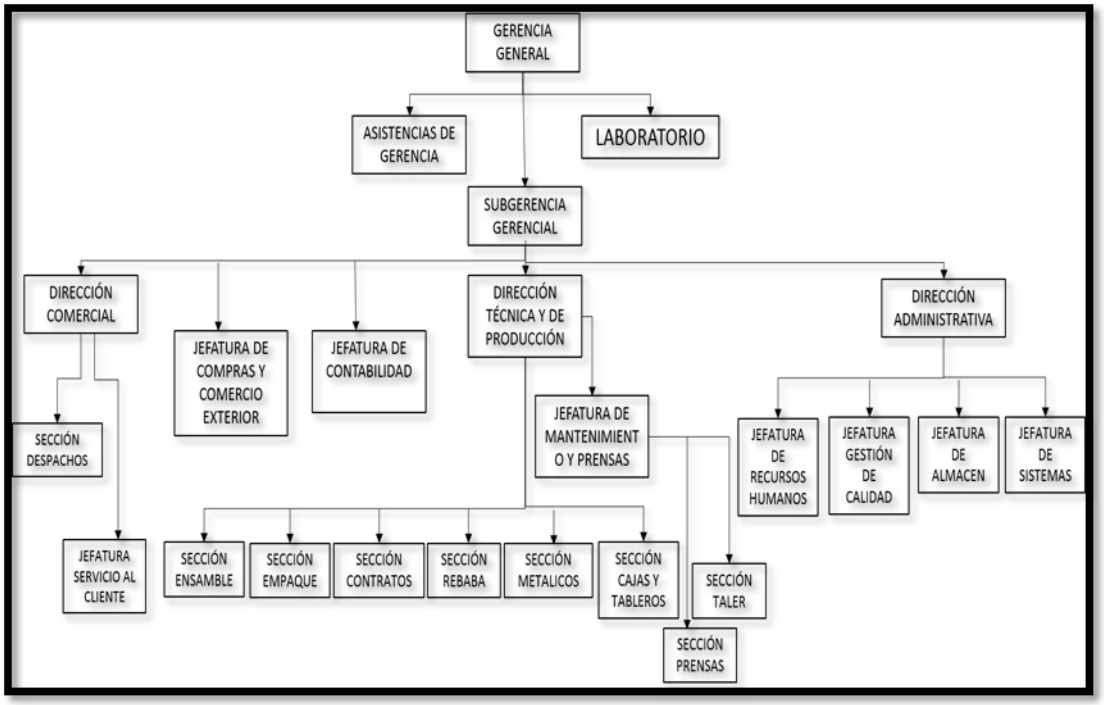
Como se puede observar en la Figura 1, la empresa cuenta con su estructura organizacional cuenta con Gerencia y Subgerencia, de la segunda Subgerencia dependen administrativamente seis (06) dependencias (Dirección Comercial, Jefatura de Compras y Comercio Exterior, Jefatura de Contabilidad, Dirección Técnica y de Producción, Dirección Administrativa).

Cada una de los niveles tiene a cargo unas áreas específicas:

Dirección Comercial (Sección Despachos – Jefatura Servicio al Cliente). Dirección Técnica y de Producción (Sección Ensamble, Empaque, Contratos, Rebaba, Metálicos, Cajas y Tableros).

Jefatura de Mantenimiento y Prensas (Sección Prensas – Sección Taller).
Dirección Administrativa (Jefatura de Recursos Humanos, Gestión de Calidad, Almacén, Sistemas).

Figura 1. Estructura organizacional.



Fuente: Empresa fabricante de productos electrónicos

6. ESTADO ACTUAL ACTIVOS

6.1 ACTIVOS DE HARDWARE

De acuerdo con la norma ISO 27001, en la cual establece la importancia de generar un inventario de activos de información, se procedió en hacer una identificación real de mencionados elementos, considerando que los activos son de alto valor para la organización, siempre y cuando exista una correlación con los sistemas de información. Ver Cuadro 2 (Descripción de activos de hardware)

Cuadro 2. Descripción de activos de hardware

Item	Descripción	Cantidad	Ubicación
1	Equipos de Cómputo de los 32 4 son Core 2 duo con 2 Gb de memoria y discos inferiores a 500gb, Windows 7.	4	Distribuidos en Ave Colombiana S.A.S
	Equipo de Computo son Core i3 hasta Core i7 con 4 gb de memoria y discos superiores o iguales a los 500gb. Windows 7.	28	Distribuidos en Área Administrativa y Operativa Ave Colombiana S.A.S – 3 bodega
2	Portátiles, Sistema Operativo Win 7, office 2013	6	1 Gerencia – 1 Subgerencia – 1Sala de reuniones – 1 Bodega
3	Servidor PowerEdge con 1TB de disco en Raid 1 para almacenamiento de datos y 600Gb en Raid 1 en sistema operativo y base de datos, con procesador xeon y 16Gb de memoria. este servidor es solo para SAP, con SQL server 2008R2, sistema operativo windows server 2008R2 y office Basic 2010 licenciados.	1	Jefatura de Sistemas
4	Fotocopiadora kyocera MFP 3040	1	Distribuidas en toda Ave Colombiana S.A.S
	Impresoras kyocera FS-2000D	2	
	Impresora kyocera FS-2020D	1	
	Impresora kyocera FS-1920	1	
	Impresora kyocera FS-2100DN	1	
	Impresora multifuncional HP K5400 officeJet	1	
	Impresora HP P1006 officeJet	1	
	Impresora multifuncional Escaner Fax Panasonic	1	
	Impresoras Matricial Epson 2190	3	
	Impresora Epson matricial lx 300	1	
5	Routher Cisco	1	Área de Diseño y Mapoteca Ave Colombiana S.A.S
6	Modem Cisco	1	
7	Firewall Astaro UTM 230 de 1gb de memoria	1	
8	Rack de Datos	1	Almacén
9	UPS	2	Área Operativa
10	Cableado UTP Categoría 5 y 6		Toda Ave Colombiana S.A.S

Fuente: Autores

El cuadro 2, refleja la información de Hardware que tiene actualmente la empresa para brindar los servicios requeridos.

6.2 ACTIVOS DE SOFTWARE

Cuadro 3. Descripción de activos software

Item	Descripción	Cantidad	Ubicación
1	Las licencias de SAP: Profesional: 7 Logistica: 11 Financiera: 3	21	Contabilidad
2	Licencias Sistema Operativo y Windows	38	Distribución Área Administrativa y Operativa
3	Bases de Datos Avecol – Avecolext -	3	Servidor – Jefatura de Sistemas

Fuente: Autores

El Cuadro 3. Refleja el software usado para el Control Financiero, Logística y Profesional, el cual es usado para mantener registro de todas las actividades de su competencia.

6.3 ACTIVOS LÓGICOS

Cuadro 4. Descripción de activos lógicos.

Item	Descripción	Cantidad	Ubicación
3	Bases de Datos Avecol – Avecolext -	3	Servidor – Jefatura de Sistemas

Fuente: Autores

El Cuadro 4, refleja la información lógica que usa para el control administrativo, de acuerdo a sus funciones.

7. APLICACIÓN ENCUESTA DIAGNÓSTICO

Con el propósito de saber, realmente, que tan importante es el tema de seguridad de la información para el personal; se aplicó una encuesta que permitió identificar varios aspectos importantes, garantizando con este resultado, que se evidencia en el mapa de riesgos es afirmativo.

Se aplicó una muestra a 31 personas que equivale al 75% de la población que posee un usuario, con acceso directo a la red.

7.1 RESULTADOS ENCUESTA REALIZADA

Teniendo en cuenta la encuesta realizada se procedió a realizar un análisis de los resultados obtenidos, que se predeterminaron valores para cada pregunta de tipo cerrado, cada una de las preguntas, tienen dos opciones de respuesta, al ser verdadera se le da el valor de uno (01) o por el contrario el valor es dos (02), valores que se consolidaron en el Cuadro No 1 (Consolidado encuesta de diagnóstico de seguridad informática).

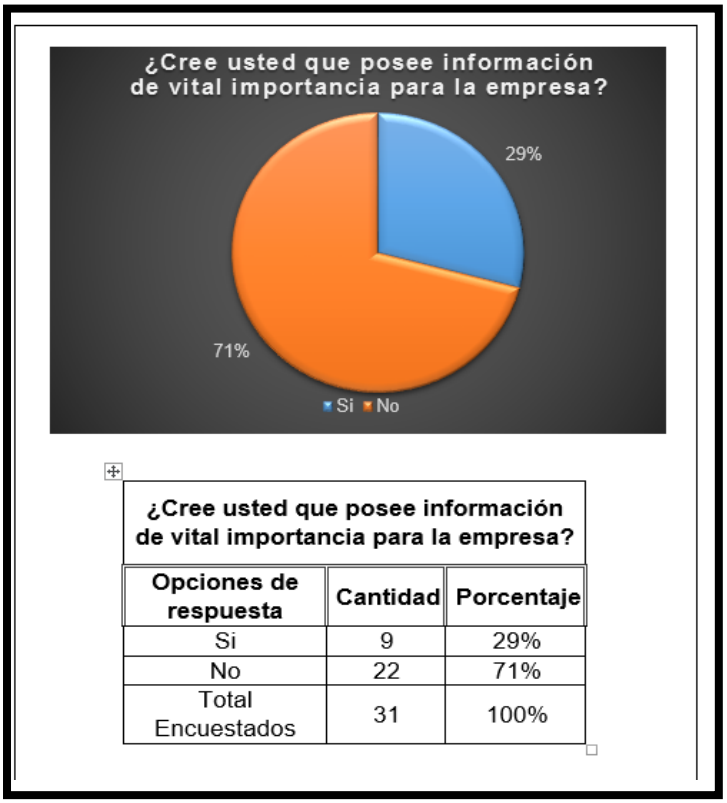
De tal manera que la encuesta que se aplicó pretendía específicamente identificar si el recurso humano, ha sido incluido con anterioridad en un programa de sensibilización en cuanto a la seguridad de la información. Evidenciándose los resultados en el Cuadro 1. Consolidado encuesta diagnóstico de seguridad informática que nunca han sido objeto de análisis y estudio, que permita de tal manera hacerlos participe del cambio al interior.

7.2 ENCUESTA REALIZADA A USUARIOS

Se realizó un cuestionario compuesto por (21 preguntas de tipo cerrado) que tiene como objetivo aplicarlo a los funcionarios de la empresa para conocer detalladamente el estado en que se encuentra cada jefatura en respecto a seguridad de la información, además poder establecer qué tipo de controles se pueden aplicar.

7.2.1 ¿Cree usted que posee información de vital importancia para la empresa?

Figura 2. Resultado estadístico pregunta No. 1



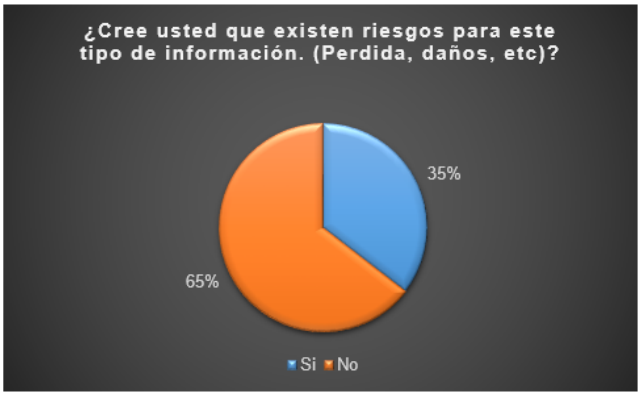
¿Cree usted que posee información de vital importancia para la empresa?		
Opciones de respuesta	**Cantidad**	**Porcentaje**
Si	9	29%
No	22	71%
Total Encuestados	31	100%

Fuente: Autores

Teniendo en cuenta con la Figura 2. se puede observar que el 71% de los encuestados desconocen si poseen información sensible de la entidad; esto permite indicar que el numeral A.7 (Seguridad de los Recursos Humanos) del anexo A de la norma ISO 27001:2013 se esta incumpliendo.

7.2.2 ¿Cree usted que existen riesgos para este tipo de información (Pérdida, daños, etc.)?

Figura 3. Resultado estadístico pregunta No 2



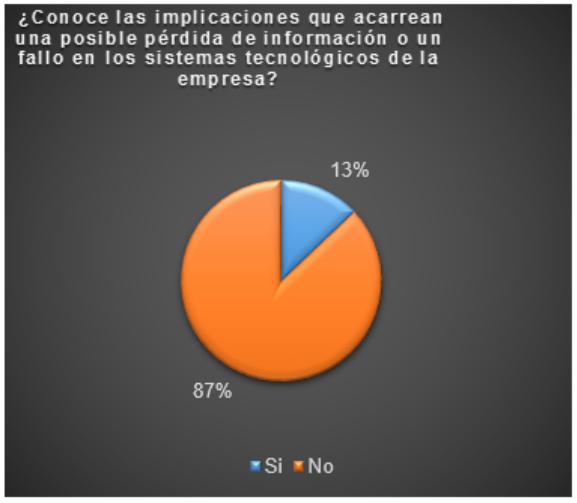
¿Cree usted que existen riesgos para este tipo de información. (Perdida, daños, etc)?		
Opciones de respuesta	**Cantidad**	**Porcentaje**
Si	11	35%
No	20	65%
Total Encuestados	31	100%

Fuente: Autores

Teniendo en cuenta la Figura 3. se puede observar que el 65% de los encuestados desconocen los riesgos que existen en la compañía frente a la información que se maneja; esto permite indicar que el numeral A11(seguridad física y de ambiente) de la norma ISO 27001:2013 se esta incumpliendo.

7.2.3 ¿Conoce las implicaciones que acarrean una posible pérdida de información o una falla en los sistemas tecnológicos de la empresa?

Figura 4. Resultado estadístico pregunta No. 3



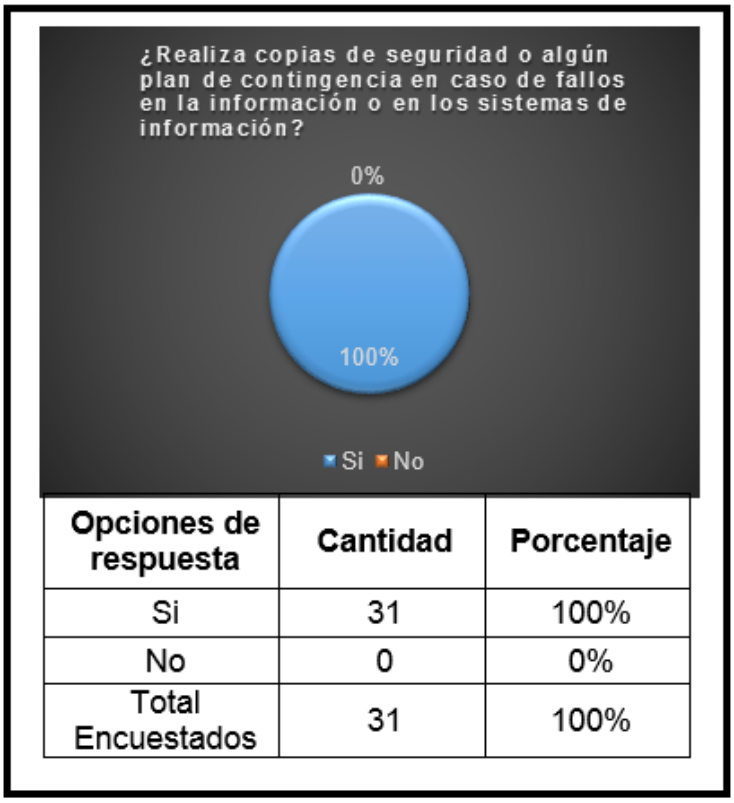
Opciones de respuesta	Cantidad	Porcentaje
Si	4	13%
No	27	87%
Total Encuestados	31	100%

Fuente: Autores.

En relación a la Figura 4 se puede observar que el 87% de los encuestados desconocen las implicaciones que conlleva la pérdida de información y/o falla del sistema de la empresa; incumpliendo todos los numerales de la norma ISO 27001:2013.

7.2.4 ¿Realiza copias de seguridad o algún plan de contingencia en caso de fallos en la información o en los sistemas de información?

Figura 5. Resultado estadístico pregunta No. 4



Opciones de respuesta	Cantidad	Porcentaje
Si	31	100%
No	0	0%
Total Encuestados	31	100%

Fuente: Autores

De acuerdo con la Figura 5. se puede observar que el 100% de los encuestados realizan copias de seguridad y poseen planes de contingencia, pero aún así presentan fallas frente al numeral A.12 (seguridad en operaciones.) del anexo A de la norma ISO 27001:2013 Teniendo en cuenta que se evidencia que el personal posee conocimiento muy vagos sobre los mecanismos de seguridad y por ende no es contemplado en su totalidad.

7.2.5 ¿Conoce usted de cuántos ordenadores dispone su empresa?

Figura 6. Resultado estadístico pregunta No. 5

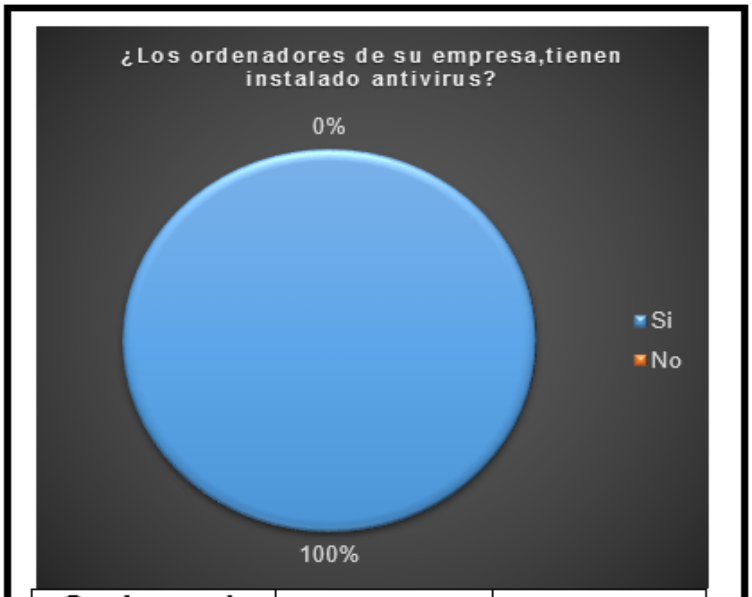
Opciones de respuesta	Cantidad	Porcentaje
Si	3	10%
No	28	90%
Total Encuestados	31	100%

Fuente: Autores.

Teniendo en cuenta la Figura 6. se puede observar que el 90% de los encuestados desconocen los activos que posee la empresa; incumpliendo el numeral A.8 (Gestiòn de Activos) del Anexo A de la norma ISO 27001:2013.

7.2.6 Los ordenadores de su empresa, ¿tienen instalado antivirus?

Figura 7. Resultado estadístico pregunta No. 6



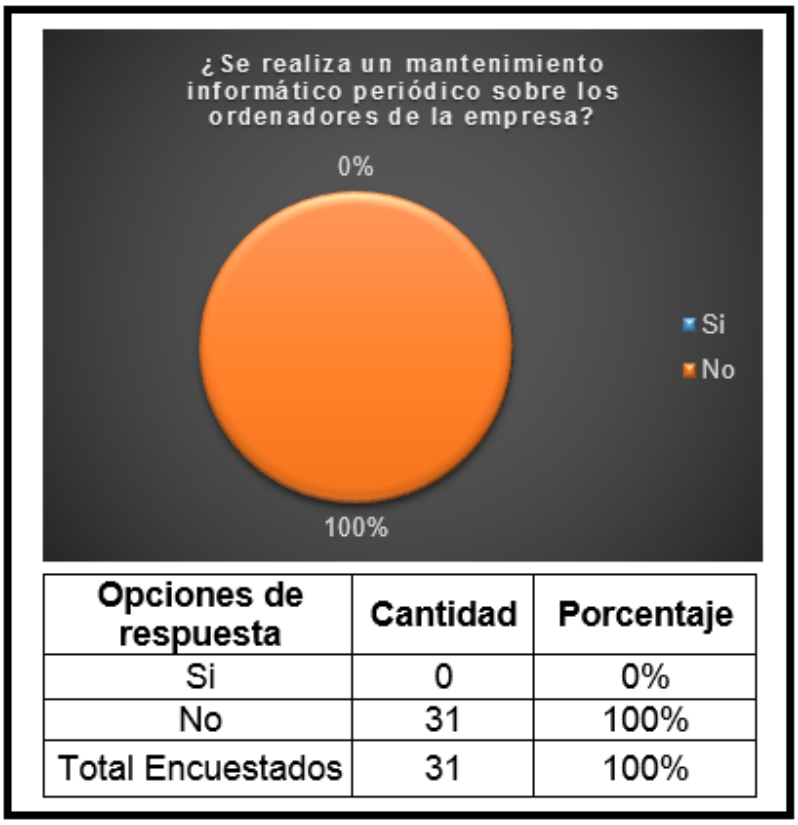
Opciones de respuesta	Cantidad	Porcentaje
Si	31	100%
No	0	0%
Total Encuestados	31	100%

Fuente: Autores.

Teniendo en cuenta la Figura 7, se puede observar que el 100% de los encuestados poseen en sus ordenadores antivirus; se identifica que se cumplen con algunos de los controles pero no satisfactoriamente, por lo tanto se deben generar cambios para el cumplimiento del numeral A.12.(seguridad en las operaciones) del Anexo A norma ISO 27001:2013).

7.2.7 ¿Se realiza un mantenimiento informático periódico sobre los ordenadores de la empresa?

Figura 8. Resultado estadístico pregunta No. 7



Opciones de respuesta	Cantidad	Porcentaje
Si	0	0%
No	31	100%
Total Encuestados	31	100%

Fuente: Autores

En relación con la Figura 8, se puede observar que el 100% de los encuestados no cuenta con un procedimiento para el mantenimiento de equipos, dado que solo se revisan cuando existe el requerimiento, es por esto que según el numeral A.11 (seguridad física y ambiental) del Anexo A de la norma ISO 27001:2013.

7.2.8 ¿Disponen de servidor central de datos en su empresa?

Figura 9. Resultado estadístico pregunta No. 8

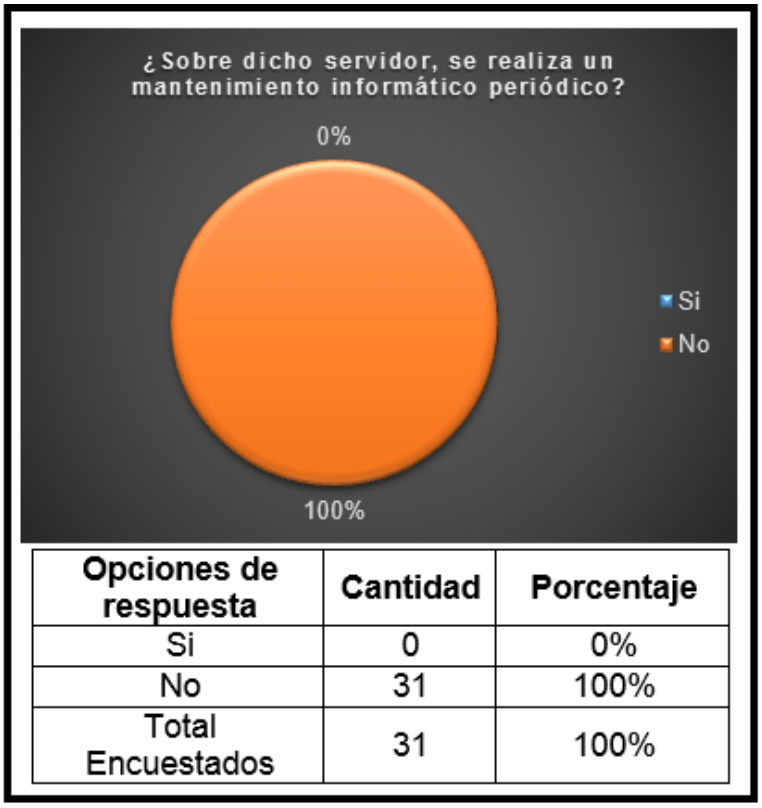
Opciones de respuesta	Cantidad	Porcentaje
Si	15	48%
No	16	52%
Total Encuestados	31	100%

Fuente: Autores.

De acuerdo con la Figura 9, se puede observar que el 52% de los encuestados manifiesta que tiene conocimiento de la existencia de los servidores pero no conoce la importancia de asegurar este activo y el 48% indica desconer la exitencia de algun tipo de servidor. Lo que genera incumpliendo del numeral A.8 (seguridad física y ambiental) del Anexo A de la norma ISO 27001:2013.

7.2.9 Sobre dicho servidor, ¿Se realiza un mantenimiento informático periódico?

Figura 10. Resultado estadístico pregunta No. 9



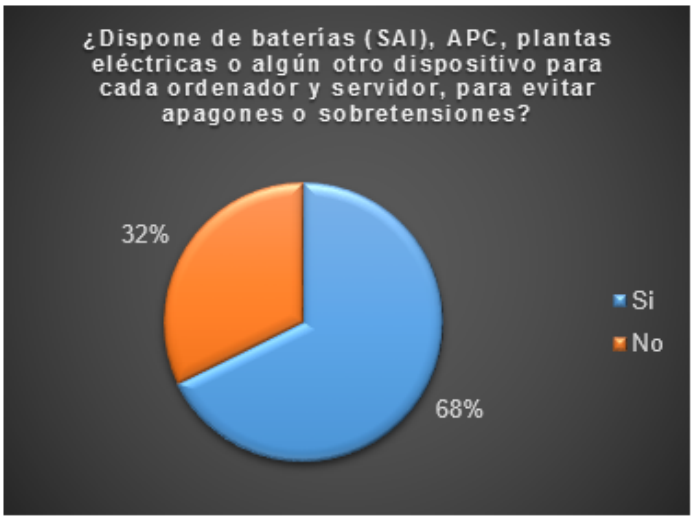
Opciones de respuesta	Cantidad	Porcentaje
Si	0	0%
No	31	100%
Total Encuestados	31	100%

Fuente: Autores.

Teniendo en cuenta la Figura 10. se puede observar que el 100% de los encuestados manifiestan que desconocen si se realiza mantenimiento informático periódico a los servidores, lo que permite establecer incumpliendo del numeral A.11 (seguridad física y ambiental) del Anexo A de la norma ISO 27001:2013

7.2.10 ¿Dispone de baterías (SAI), APC, plantas eléctricas o algún otro dispositivo para cada ordenador y servidor, para evitar apagones o sobretensiones?

Figura 11. Resultados estadísticos preguntas No. 10



Opciones de respuesta	Cantidad	Porcentaje
Si	21	68%
No	10	32%
Total Encuestados	31	100%

Fuente: Autores.

Teniendo en cuenta la Figura 11. se puede observar que el 68% de los encuestados manifiestan conocer la existencia de una planta eléctrica, debido a la falta de sensibilizaciòn en cuanto al tema de seguridad de la información. indicando que se incumple el numeral de A.11 (seguridad fisica y el ambiente) del Anexo A de la norma ISO 27001:2013.

7.2.11 ¿Conoce usted si la empresa tiene políticas de seguridad informática?

Figura 12. Resultado estadístico pregunta No. 11

Opciones de respuesta	Cantidad	Porcentaje
Si	0	0%
No	31	100%
Total Encuestados	31	100%

Fuente: Autores.

En relación con la Figura 12 se puede observar que el 100% de los encuestados manifiestan que no posee una politica de seguridad de la informaciòn; estableciendo el incumplimiento el numeral A.5 (Politicas de seguridad de la información). del Anexo A de la norma ISO 27001:2013.

7.2.12 ¿Cuenta con un plan de contingencia en caso de un desastre natural o un mal manejo de información?

Figura 13. Resultado estadístico pregunta No.12

Opciones de respuesta	Cantidad	Porcentaje
Si	14	45%
No	17	55%
Total Encuestados	31	100%

Fuente: Autores.

De acuerdo con la Figura 13, se puede observar que el 55% de los encuestados manifiestan que no se cuenta con un Plan de Contingencia en caso de un desastre natural. Entendiendo que la empresa maneja sus backup, el lugar de su almacenamiento no es el indicado dado que las copias de la información se encuentran en la misma planta y en el mismo lugar de quienes los generan. Incumpliendo el numeral A.16 (Gestión de incidentes de seguridad de la información) y en el numeral A.17. (Aspectos de seguridad de la información de la gestión de la continuidad de negocio).de la norma ISO 27001:2013.

7.2.13 ¿Conoce usted de los riesgos informáticos a los que están expuestos?

Figura 14. Resultados estadístico pregunta No.13

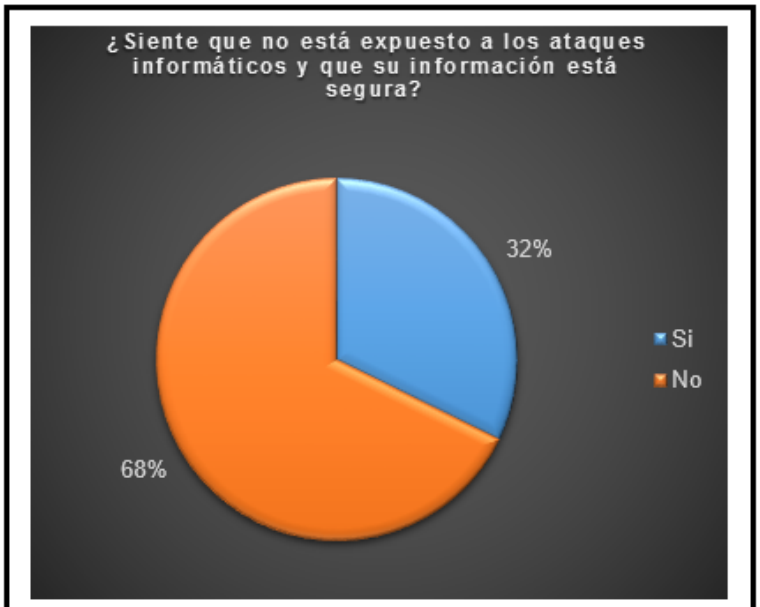
Opciones de respuesta	Cantidad	Porcentaje
Si	16	52%
No	15	48%
Total Encuestados	31	100%

Fuente: Autores.

Teniendo en cuenta la Figura 14, se puede observar que el 52% de los encuestados manifiestan saber de los riesgos informaticos a los que estan expuestos. Esta pregunta apunta al incumplimiento de los numerales A6 (Organización de la seguridad de la información), A7 (Seguridad de los recursos humanos), A11 (Seguriad fisica y del entorno), A12 (Seguridad de las operaciones), A15 (Relaciones con los proveedores), A16 (Gestion de los incidentes de suguridad de la información), A17 (redundancias).de la norma ISO 27001:2013.

7.2.14 ¿Siente que no está expuesto a los ataques informáticos y que su información está segura?

Figura 15. Resultados estadístico pregunta No. 14



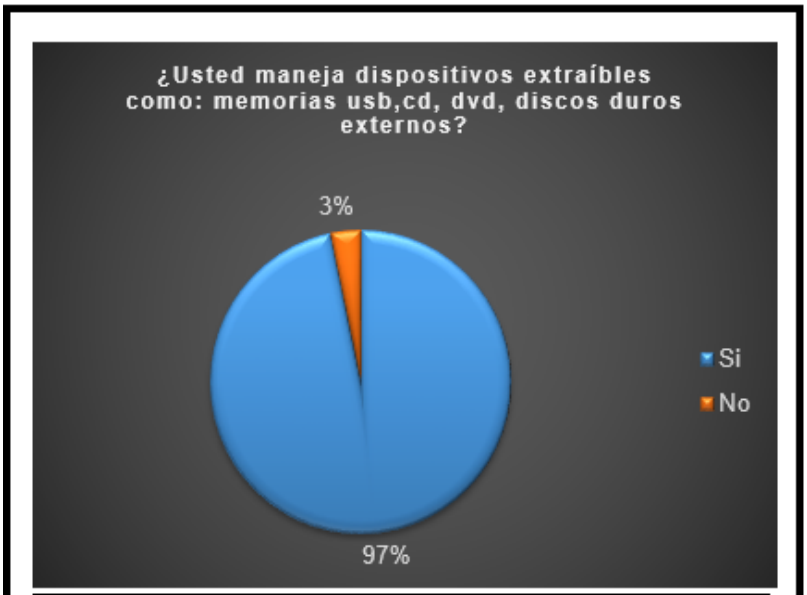
Opciones de respuesta	Cantidad	Porcentaje
Si	10	32%
No	21	68%
Total Encuestados	31	100%

Fuente: Autores

Teniendo en cuenta la Figura 15, se puede observar que el 68% de los encuestados manifiestan que a pesar de conocer el concepto de amenazas informaticas no estan expuestos a ataques debido a que cuentan con un firewall y antivirus, que los protege de cualquier incidente, incumplimiento . Esta pregunta apunta al incumplimiento del numeral A8 (gestión de activos) del Anexo A de la norma ISO27001:2013.

7.2.15 ¿Usted maneja dispositivos extraíbles como: memorias USB, CD, DVD, discos duros externos?

Figura 16. Resultados estadístico pregunta No. 15



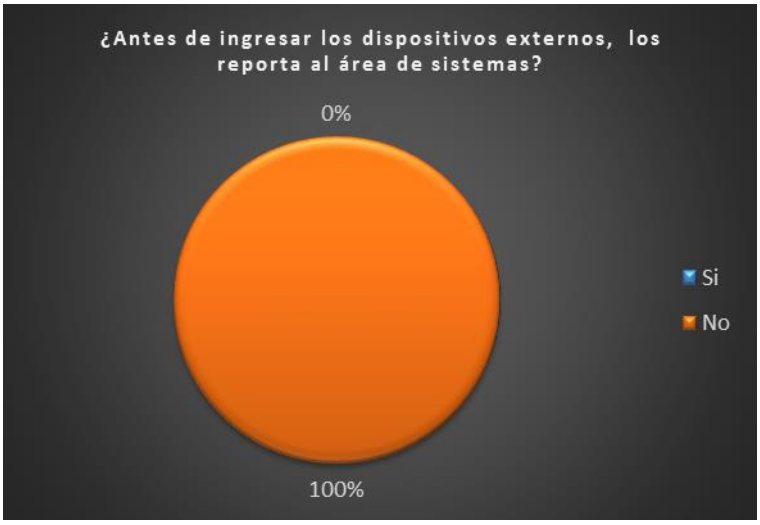
Opciones de respuesta	Cantidad	Porcentaje
Si	30	97%
No	1	3%
Total Encuestados	31	100%

Fuente: Autores

Teniendo en cuenta la Figura 16, se puede observar que el 97% de los encuestados manifiestan que manena dispositivos extraibles en la empresa, indicando que los mismos son elementos que hacen parte de su labor, lo que refleja la no existencia de politicas de seguridad para el manejo de los medios de almacenamiento. Incumplimiendo los numerales del Anexo A de la norma A6 (Políticas de Seguridad de la Información), A16 (Gestión de Incidentes de Seguridad de la Informacion).

7.2.16 ¿Antes de ingresar los dispositivos externos, los reporta al área de sistemas?

Figura 17. Resultados estadístico pregunta No. 16



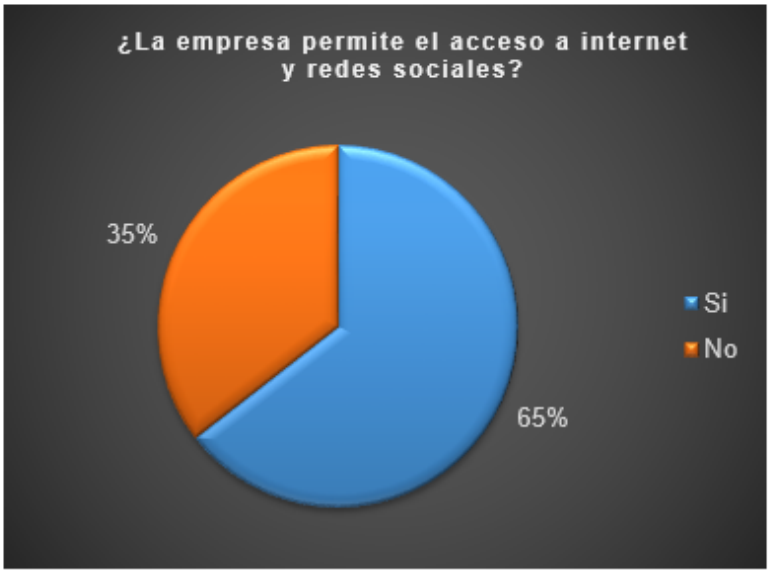
Opciones de respuesta	Cantidad	Porcentaje
Si	31	100%
No	0	0%
Total Encuestados	31	100%

Fuente: Autores

Teniendo en cuenta la Figura 17, se puede observar que el 100% de los encuestados manifiestan que ingresan dispositivos externos a la entidad sin informar al área de sistemas. Haciendo de los sistemas informaticos vulnerables a ataques informáticos, fuga de información. Incumplimiendo el numeral A9 (Control de Acceso) del Anexo A de la norma ISO 27001:2013.

7.2.17 ¿La empresa permite el acceso a internet y redes sociales?

Figura 18. Resultados estadístico pregunta No. 17



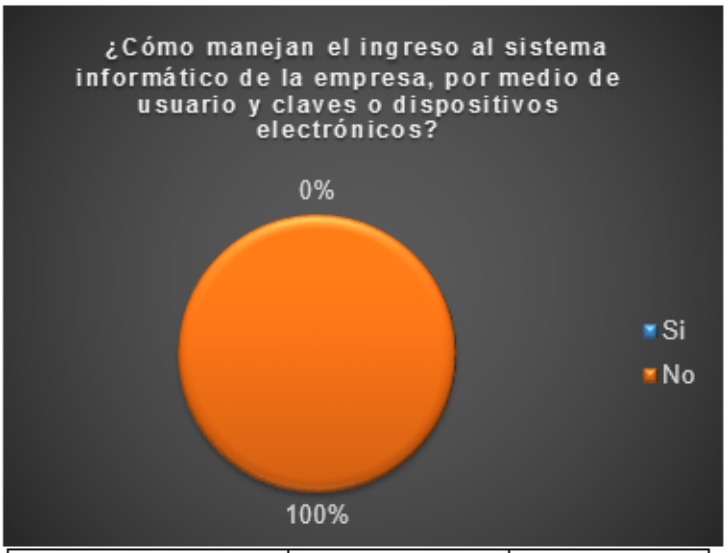
Opciones de respuesta	Cantidad	Porcentaje
Si	20	65%
No	11	35%
Total Encuestados	31	100%

Fuente: Autores

En relación con la Figura 18, se puede observar que el 65% de los encuestados manifiestan que tienen acceso a internet más no a redes sociales, dado que el acceso a las mismas son limitadas. Esta pregunta apunta al numeral A9 (control de acceso) del Anexo de la norma ISO 27001:2013, el cual no esta siendo contemplando

7.2.18 ¿Cómo manejan el ingreso al sistema informático de la empresa, por medio de usuario y claves o dispositivos electrónicos?

Figura 19. Resultados estadístico pregunta No. 18



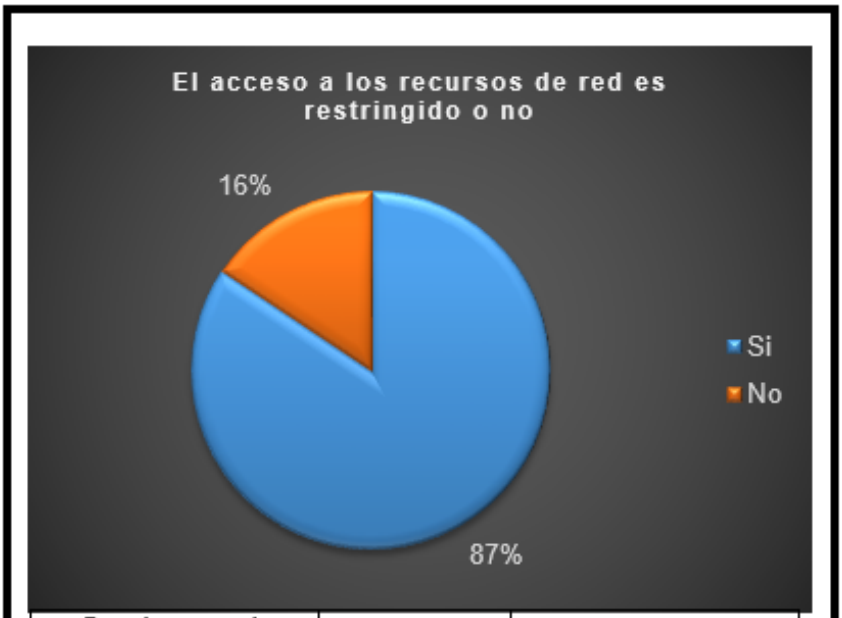
Opciones de respuesta	Cantidad	Porcentaje
Si	0	0%
No	31	100%
Total Encuestados	31	100%

Fuente: Autores

De acuerdo con la Figura 19, se puede observar que la mayoria de los encuestados manifiestan no poseer o manejar claves de acceso al sistemas por medio de dispositivos electronicos, incumpliendo el numeral A9 (control de acceso) del Anexo A de la norma ISO 27001:2013.

7.2.19 ¿El acceso a los recursos de red es restringido o no?

Figura 20. Resultados estadístico pregunta No. 19



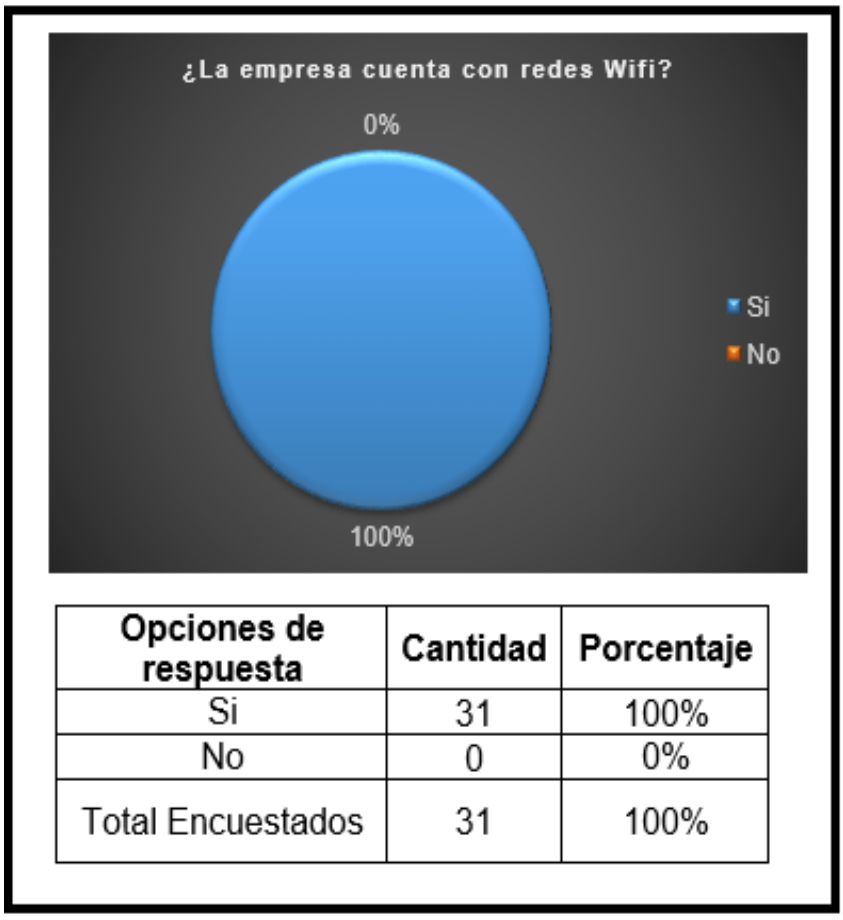
Opciones de respuesta	Cantidad	Porcentaje
Si	27	87%
No	5	16%
Total Encuestados	31	100%

Fuente: Autores

Teniendo en cuenta la Figura 20 se puede observar que el 87% de los encuestados no poseen acceso a la red y son restringidos por medio del Firewall. incumpliendo el numeral A9 (control de acceso) del Anexo A de la norma ISO 27001:2013.

7.2.20 ¿La empresa cuenta con redes Wi-Fi?

Figura 21. Resultados estadístico pregunta No. 20



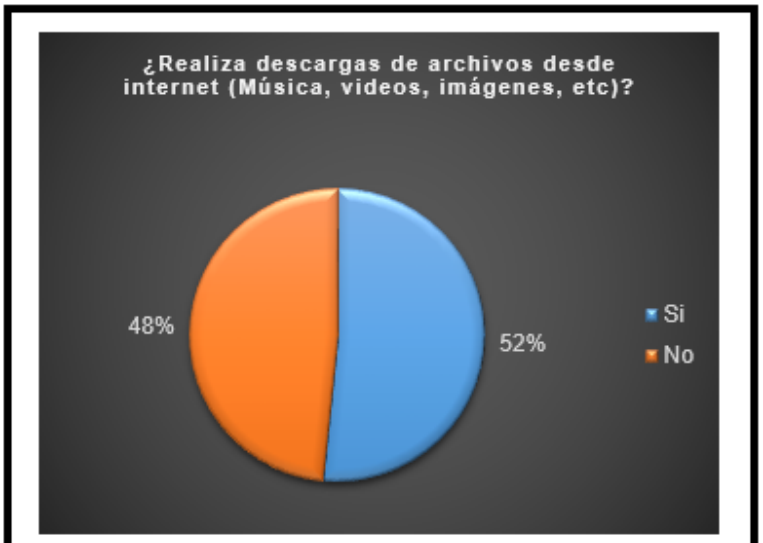
Opciones de respuesta	Cantidad	Porcentaje
Si	31	100%
No	0	0%
Total Encuestados	31	100%

Fuente: Autores.

Teniendo en cuenta la Figura 21 se puede observar que cuenta con una red Wi-Fi la cual tiene restricciones. incumpliendo el numeral A9 (control de acceso) A13 (seguridad de las comunicaciones), A15 (relaciones con los proveedores) los cuales no estan siendo contemplandos del Anexo A de la norma ISO 27001:2013.

7.2.21 ¿Realiza descargas de archivos desde internet (Música, videos, imágenes, etc.)?

Figura 22. Resultados estadístico pregunta No. 21



Opciones de respuesta	Cantidad	Porcentaje
Si	16	52%
No	15	48%
Total Encuestados	31	100%

Fuente: Autores.

Teniendo en cuenta la Figura 22 se puede observar que el 52% de los encuestados descarga música, imágenes, videos y otra información. Debido a que la empresa no cuenta con un directorio activo para realizar el bloqueo necesario para evitar este tipo de descargas. Incumpliendo A9(control de acceso), A13 (Seguridad de las Comunicaciones), A14 (Adquisición, Desarrollo y Mantenimiento de Sistemas) del Anexo A de la norma ISO 27001:2013.

8. VERIFICACIÓN Y APLICACIÓN DE LA NORMA ISO 27001:2013

Con el fin de realizar una propuesta adecuada se llevó a cabo una visita de campo, que permitió identificar los daños y el impacto de incidentes de seguridad. El análisis de riesgo se requiere para establecer que activos están bajo riesgo, logrando con esto que la Alta Gerencia tome decisiones y definiendo cuales serán aceptados y que mecanismos serán aplicados en búsqueda de mitigar eficientemente estos riesgos.

Teniendo en cuenta lo anterior, se da inició a la evaluación de los numerales del Anexo A de la norma ISO 27001:2013. Así mismo, y con el propósito de mantener un orden de los hallazgos encontrados por numeral, se designó un número consecutivo para lograr coherencia en los resultados.

8.1 MATRIZ DE RIESGOS Y ACCIONES MITIGANTES

Durante el proceso de recolección de información, y como mecanismo para hallar los riesgos, se realizó una matriz de riesgos y las acciones mitigantes, que permitió documentar los numerales que están siendo incumplidos y/o cumplidos; luego ubicar la información en Zonas de Riesgos, para facilitar su consulta.

8.1.1 Valoración del riesgo

Cuadro 5. Valores de riesgo

Probabilidad	Valor	Zonas de Riesgo		
3	Alta	15 Moderado	30 Importante	60 Inaceptable
2	Media	10 Tolerable	20 Moderado	40 Importante
1	Baja	5 Aceptable	10 Tolerable	20 Moderado
	Impacto	Leve	Moderada	Catastrófica
	Valor	5	10	20

Fuente: Autores.

En esta parte del proyecto, el proceso de identificación de los riesgos se contempló manejar el Cuadro 5 Valores del riesgo. El uso de este cuadro permitió establecer en qué estado se encuentra bajo la norma ISO 27001:2013. Consiste en la verificación de la probabilidad en que ocurra el evento Vs el impacto de ocurrencia del evento y la criticidad del riesgo. La multiplicación de estas dos variables, se obtuvo un resultado, el cual se ubicó en las zonas de riesgo.

Cada una de las zonas de riesgo tiene un tratamiento especial para los riesgos encontrados:

Inaceptable: corresponde al nivel de riesgo más alto y el cual contempla que los riesgos encontrados deben ser controlados de manera inmediata, capaz de prevenir, reducir, transferir o compartir el riesgo.

Importante: corresponde a un nivel de riesgo más alto y el cual contempla que los riesgos encontrados deben ser controlados de manera inmediata, capaz de prevenir, reducir, transferir o compartir el riesgo.

Moderado: Deben ser tratados con un fin, evitarlos.

Tolerable: corresponde a un nivel permisible, de tal manera que se deben monitorear para que se reduzcan eficientemente.

Aceptable: corresponde a nivel en el cual se deben monitorear para que los riesgos no pasen a un nivel de criticidad superior.

8.1.2 Matriz de riesgos

La presente matriz de riesgos, fue diseñada basándose en la norma ISO 27001-2013 y los valores de riesgo establecidos anteriormente; por lo tanto, se correlaciono los dos instrumentos de tal forma que permitio obtener el impacto real de incumplimiento de los objetivos de control establecidos en la norma. Así mismo, identificar los riesgos que tiene la empresa y que no están siendo tratados, por la falta de un sistema de gestión y seguridad de la información adecuado.

Cuadro 6. Matriz de Riesgo

Vulnerabilidad	Descripción vulnerabilidad	Consecuencia	Control	Responsable	Ejecutante	Probabilidad vs impacto
Políticas para la seguridad la información.	Desconocimiento de la importancia de la seguridad de la información.	Des aseguramiento de la información	Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y partes interesadas.	Alta dirección - Área de sistemas de ave	Área de sistemas ave	60
		Incumplimiento a los parámetros establecidos externos e internos que el sistema proporcional.	Concientizar a la alta dirección la importancia de implementar un sistema de gestión de la seguridad de la información	Área de sistemas ave	Área de sistemas ave	60
Organización de la seguridad de la información.	Falta de establecer roles y responsabilidades.	Mal manejo de la información por el personal.	Se deben definir y asignar todas las responsabilidades de la seguridad de la información.	Área de sistemas ave	Área de sistemas ave	20
	Se evidencia que se realizan actividades propias del área de sistemas en áreas ajenas a ella.	No hay responsables - pérdida de información	Separación de deberes. Las tareas y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional o el uso indebido de los activos de la organización.	Área de sistemas ave	Área de sistemas ave	20

Cuadro 6. Continuación

Vulnerabilidad	Descripción vulnerabilidad	Consecuencia	Control	Responsable	Ejecutante	Probabilidad vs impacto
Organización de la seguridad de la información.	No se evidencia contacto con autoridades pertinentes.	No se realiza el proceso de estudio para el personal que labora	Se debe mantener contactos apropiados con las autoridades pertinentes.	Área de sistemas ave	Área de sistemas ave	10
	No se evidencia contacto con autoridades pertinentes	Desconocimiento de temas asociados al tema de seguridad - no existe un medio para retroalimentar fallas	Se deben mantener controles apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.	Área de sistemas ave	Área de sistemas ave	20
	Acceso de dispositivos móviles sin restricción	Altos riesgos inducidos por uso de dispositivos móviles	Política para dispositivos móviles. Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	Área de sistemas ave	Área de sistemas ave	30
	No se evidencia una política y medidas de seguridad para salvaguardar la información	Pérdida de información vulnerable - imagen empresarial	Teletrabajo. Se deben implementar una política y medidas de seguridad de soporte para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.	Área de sistemas ave	Área de sistemas ave	30
Seguridad de los recursos humanos.	No se realiza el proceso de estudio para el personal que labora	Extracción de información correspondiente al nivel de clasificación de la información	Selección. Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes,	Área de sistemas ave	Área de sistemas ave	60

Cuadro 6. Continuación

Vulnerabilidad	Descripción vulnerabilidad	Consecuencia	Control	Responsable	Ejecutante	Probabilidad vs impacto
Seguridad de los recursos humanos.			reglamentos y ética pertinentes, y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.			60
	No evidencia la aplicación de la seguridad para los empleados ni los contratistas.	Extracción de información correspondiente al nivel de clasificación de la información	La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos de la organización.	Dirección, área de sistemas y área recursos humanos	área de sistemas y área recursos humanos	60
	Falta de capacitación para el personal que hace parte de los procesos	Desconocimiento - posible fuga de información - perjuicio para la imagen empresarial.	Toma de conciencia, educación y formación de la seguridad de la información. Todos los empleados de la organización y donde sea pertinente, los contratistas deben recibir educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.	área de sistemas y área recursos humanos	área de sistemas y área recursos humanos	30

Cuadro 6. Continuación

Vulnerabilidad	Descripción vulnerabilidad	Consecuencia	Control	Responsable	Ejecutante	Probabilidad vs impacto
Seguridad de los recursos humanos.	No se evidencia de la existencia de un proceso que establezca acciones formales en el caso de violentar algunos de los sistemas de seguridad.	Desconocimiento de la Ley.	Proceso disciplinario. Se debe contar con un proceso formal y comunicado para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	área de sistemas y Área recursos humanos - área jurídica	área de sistemas y área recursos humanos - área jurídica	30
	No se evidencia la existencia proceso y/o métodos para informar la terminación o cambio de responsabilidad de empleo.	No hay compromiso ni responsabilidad del empleado.	Terminación o cambio de responsabilidades de empleo. Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo se deben definir, comunicar al empleado o contratista y se deben hacer cumplir.	área de sistemas y área recursos humanos	área de sistemas y área recursos humanos	10
Gestión de activos.	No se evidencia la existencia de un inventario de activos	Información no confiable de los activos - no existencia de cronograma de mantenimiento	Inventario de activos. Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.	área de sistemas - área almacén	área de sistemas - área almacén	60
	No se evidencia proceso verificación de activos en calidad de prestamos	desconocimiento de los equipos que no son propios - ni proceso para los mismo	Propiedad de los activos. Los activos mantenidos en el inventario deben ser propios.	área de sistemas	área de sistemas	30

Cuadro 6. Continuación

Vulnerabilidad	Descripción vulnerabilidad	Consecuencia	Control	Responsable	Ejecutante	Probabilidad vs impacto
Gestión de activos.	No se evidencia la existencias de mecanismos quede a conocer cuál es la manera adecuada de manipular los activos	Deterioro de los activos - pérdida de tiempo en las labores propias - aumento de costos	Uso aceptable de los activos. Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	Área de sistemas	Área de sistemas	30
	No se evidencia la existencia de un proceso de devolución de activos para los empleados de ave.	Aumento en la desviación de los activos - aumento de las necesidades tecnológicas - Pérdida de información.	Devolución de Activos. Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	Área de Sistemas - Área Almacén	Área de Sistemas - Área Almacén	30
	No se evidencia clasificación de la información	Divulgación de información por personal no autorizado	Clasificación de la información. La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	Área de sistemas	Área de sistemas	30

Cuadro 6. Continuación

Vulnerabilidad	Descripción vulnerabilidad	Consecuencia	Control	Responsable	Ejecutante	Probabilidad vs impacto
Gestión de activos.	Se evidencia que existe un proceso para el manejo de los activos	Control con los activos	Manejo de activos. Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	Área de sistemas - área almacén	Área de sistemas - área almacén	5
	No se evidencia un tratamiento para los medios de soporte removibles	Fuga de información - Pérdida de datos	Gestión de medios de soporte removibles. Se deben implementar procedimientos para la gestión de medios de soporte removibles, de acuerdo con el esquema de clasificación adoptado por la organización.	Área de sistemas	Área de sistemas	60
	No se evidencia un mecanismo para la disposición de los medios de soporte	Fuga de información - falta de control de los activos	Disposición de los medios de soporte. Se debe disponer en forma segura de los medios de soporte cuando ya no se requieran, utilizando procedimientos formales.	Área de sistemas - área almacén	Área de sistemas - área almacén	30
	No se evidencia de un proceso para la transferencia de medios de soporte físicos	Fuga de información - uso mal intencionado	Transferencia de medios de soporte físicos. Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	Área de sistemas	Área de sistemas	30

Cuadro 6. Continuación

Vulnerabilidad	Descripción vulnerabilidad	Consecuencia	Control	Responsable	Ejecutante	Probabilidad vs impacto
Control de acceso.	No existe política control de acceso	Desconocimiento una política de control acceso por parte del personal.	Política de control de acceso. Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	Área de sistemas	Área de sistemas	60
	No se evidencia control de acceso a la red y a los servicios	Ingreso personal no autorizado - manipulación inadecuado de la información y los servicios	Acceso a redes y a servicios en red. Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	Área de sistemas	Área de sistemas	60
	No se evidencia control del registro y cancelación de usuarios	Ingreso personal no autorizado - manipulación inadecuado de la información y los servicios	Registro y cancelación del registro de usuarios. Se debe implementar un proceso formal de registro y de cancelación del registro para posibilitar la asignación de los derechos de acceso.	Área de sistemas	Área de sistemas	30
	No se evidencia un mecanismo para el suministro de acceso a los usuarios	Fuga de información	Suministro de acceso de usuarios. Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o cancelar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.	Área de sistemas	Área de sistemas	30

Cuadro 6. Continuación

Vulnerabilidad	Descripción vulnerabilidad	Consecuencia	Control	Responsable	Ejecutante	Probabilidad vs impacto
Control de acceso.	No se evidencia un mecanismo para el suministro de acceso a los usuarios	Uso inadecuado de la información	Gestión de derechos de acceso privilegiado. Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.	Dirección, área de sistemas	Dirección, área de sistemas	30
	No se evidencia la existencia de revisiones periódicas de acceso de los usuarios	Accesos sin control. Fuga de información	Revisión de los derechos de acceso de usuarios. Los dueños de los activos deben revisar los derechos de acceso de los usuarios a intervalos regulares.	Área de sistemas	Área de sistemas	30
	Acceso de dispositivos móviles sin restricción	Acceso sin control, para el personal que es ajeno a la entidad	Cancelación o ajuste de los derechos de acceso. Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procedimiento de información se deben cancelar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.	Área de sistemas	Área de sistemas	30
	Desconocimiento de información secreta y el cuidado que deben tener los empleados	Mala manipulación y divulgación de la información	Uso de información secreta. Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	Área de sistemas	Área de sistemas	30

Cuadro 6. Continuación

Vulnerabilidad	Descripción vulnerabilidad	Consecuencia	Control	Responsable	Ejecutante	Probabilidad vs impacto
Control de acceso.	No se evidencia restricción de acceso a la información	Acceso no autorizado - modificación en las operaciones	Restricción de acceso a información. El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.	Área de sistemas	Área de sistemas	30
	No se evidencia la existencia de un procedimiento de conexión segura	Fuga de información en la transferencia	Procedimiento de conexión segura. Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de conexión segura.	Área de sistemas	Área de sistemas	60
	No se evidencia un procedimiento de gestión de contraseñas	No se aplica contraseñas de acuerdo al procedimiento	Sistema de gestión de contraseñas. Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad.	Área de sistemas	Área de sistemas	60
	No se evidencia el control sobre programas utilitarios	Anulación del sistema - denegación de servicio	Uso de programas utilitarios privilegiados. Se debe restringir y controlar estrechamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.	Área de sistemas	Área de sistemas	60

Cuadro 6. Continuación

Vulnerabilidad	Descripción vulnerabilidad	Consecuencia	Control	Responsable	Ejecutante	Probabilidad vs impacto
Control de acceso.	No se evidencia un procedimiento para el control de acceso al código fuente	Modificación de información - acceso no autorizados	Control de acceso a códigos fuente de programas. Se debe restringir el acceso a códigos fuente de programas.	Área de sistemas	Área de sistemas	60
Criptografía	No se evidencia la existencia de una política que aplique los controles criptográficos	Divulgación de la información sin control	Política sobre el uso de controles criptográficos. Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para protección de información.	Área de sistemas	Área de sistemas	30
	No se evidencia la existencia de un procedimiento de gestión de claves	Divulgación de la información sin control	Gestión de claves. Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de claves criptográficas, durante todo su ciclo de vida.	Área de sistemas	Área de sistemas	30
Seguridad física y ambiental.	No se evidencia la delimitación de perímetro de seguridad	El espacio que existe para el almacenamiento de información	Perímetro de seguridad física. Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información.	Dirección, Área de sistemas	Dirección, Área de sistemas	30

Cuadro 6. Continuación

Vulnerabilidad	Descripción vulnerabilidad	Consecuencia	Control	Responsable	Ejecutante	Probabilidad vs impacto
Seguridad física y ambiental.	La oficina de sistemas no cumple con los controles físicos de entrada	Fuga de información - alteración en las operaciones - acceso no autorizado - vandalismo	Controles físicos de entrada. Las áreas seguras se deben proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.	Dirección, Área de sistemas	Dirección, Área de sistemas	60
	La oficina de sistemas de ave, es compartida con otro usuario.	Fuga de información - alteración en las operaciones - acceso no autorizado - allanamiento ilegal	Seguridad de oficinas, salones e instalaciones. Se debe diseñar y aplicar seguridad física a oficinas, salones e instalaciones.	Área de sistemas	Área de sistemas	60
	No se evidencia la existencia de un procedimiento contra las amenazas ambientales	Pérdida de información - desestabilización del sistema	Protección contra amenazas externas y ambientales. Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	Área de sistemas	Área de sistemas	60
	No se evidencia que se coloque en práctica el tema de trabajo en áreas seguras	Pérdida de información - sabotaje (ataque físico y/o electrónico)	Trabajo en áreas seguras. Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.	Área de sistemas	Área de sistemas	5

Cuadro 6. Continuación

Vulnerabilidad	Descripción vulnerabilidad	Consecuencia	Control	Responsable	Ejecutante	Probabilidad vs impacto
Seguridad física y ambiental.	Manejo inadecuado de contraseñas (inseguras, no cambian, compartidas)	Pérdida y/o modificación de información	Áreas de despacho y carga. Se deben controlar los puntos de acceso tales como áreas de despacho y de carga y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	Área de sistemas	Área de sistemas	30
	Falta de inducción, capacitación y sensibilización de los riesgos informáticos	Pérdida de información - sabotaje (ataque físico y/o electrónico)	Ubicación y protección de los equipos. Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales y las posibilidades de acceso no autorizado.	Dirección, área de sistemas y demás áreas que intervengan	Dirección, área de sistemas y demás áreas que intervengan	30
	Falta de inducción, capacitación y sensibilización de los riesgos informáticos	Pérdida de información - sabotaje (ataque físico y/o electrónico)	Ubicación y protección de los equipos. Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales y las posibilidades de acceso no autorizado.	Dirección, área de sistemas y demás áreas que intervengan	Dirección, área de sistemas y demás áreas que intervengan	30
	Se evidencia la existencia de planta eléctrica para los equipos ups	Medio que subsana cualquier falla de corriente	Servicios públicos de soporte. Los equipos se deben proteger de fallas de potencia y otras interrupciones causadas por fallas en los servicios públicos de soporte.	Área de sistemas - área mantenimiento	Área de sistemas - área mantenimiento	30

Cuadro 6. Continuación

Vulnerabilidad	Descripción vulnerabilidad	Consecuencia	Control	Responsable	Ejecutante	Probabilidad vs impacto
Seguridad física y ambiental.	No se evidencia la existencia del procedimiento de seguridad de cableado de datos	Red cableada expuesta para el acceso no autorizado	Seguridad del cableado. El cableado de potencia y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptaciones, interferencia o daño.	Área de sistemas	Área de sistemas	30
	No se evidencia la existencia de un cronograma de mantenimiento a los activos	Se permite la disponibilidad de la información - desconocimiento de necesidades tecnológicas	Mantenimiento de equipos. Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Área de sistemas	Área de sistemas	30
	No se evidencia procedimiento para el trámite de retiro de activos	Falta de control en los activos	Retiro de activos. Los equipos, información o software no se deben retirar de su sitio sin autorización previa.	Área de sistemas - área de seguridad	Área de sistemas - área de seguridad	20
	No se evidencia procedimiento para el trámite de seguridad para los activos fuera de ave	Falta de control en los activos	Seguridad de equipos y activos fuera del predio. Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de los predios de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichos predios.	Área de sistemas - área de seguridad	Área de sistemas - área de seguridad	20

Cuadro 6. Continuación

Vulnerabilidad	Descripción vulnerabilidad	Consecuencia	Control	Responsable	Ejecutante	Probabilidad vs impacto
Seguridad física y ambiental.	No se evidencia de la existencia de un procedimiento que trate sobre los desechos electrónicos y/o reutilización de equipos	Divulgación de información - tramite inadecuado de la información - contaminación ambiental	Disposición segura o reutilización de equipos. Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software con licencia haya sido retirado o sobre escrito en forma segura antes de su disposición o reusó.	Área de sistemas	Área de sistemas	30
	Falta de inducción, capacitación y sensibilización de los riesgos informáticos	Desconocimiento - posible fuga de información - perjuicio para la imagen empresarial	Equipos sin supervisión de los usuarios. Los usuarios deben asegurarse de que el equipo sin supervisión tenga la protección apropiada.	Dirección, área de sistemas, todos los usuarios	Área de sistemas. Usuarios	20
	No se evidencia procedimiento para tratar la política de escritorio limpio y pantalla limpia - falta capacitación - desconocimiento de la norma	Información vulnerable - fuga y Pérdida de información	Política de escritorio limpio y pantalla limpia. Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia para las instalaciones de procesamiento de información.	Área de sistemas	Área de sistemas	20

Cuadro 6. Continuación

Vulnerabilidad	Descripción vulnerabilidad	Consecuencia	Control	Responsable	Ejecutante	Probabilidad vs impacto
Seguridad de las operaciones.	No se evidencia procedimiento de operaciones - y no son divulgadas a los usuarios	Desconocimiento en cuanto a la forma de seguir los procedimientos	Procedimientos de operación documentadas. Los procedimientos operativos se deben documentar y poner a disposición de todos los usuarios que los necesitan.	Área de sistemas	Área de sistemas	20
	No se evidencia gestión de cambios en ave	Por la falta de planeamiento metodológico se puede incurrir en fallas constantes	Gestión de cambios. Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	Área de sistemas	Área de sistemas	30
	No se evidencia gestión de capacidad	No se tiene información verídica para proyecciones requeridas al sistema	Gestión de capacidad. Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.	Área de sistemas	Área de sistemas	30
	La oficina de sistemas es una sola para todos los ambientes (desarrollo, ensayo y operación)	Aumento significativo para el acceso no autorizado para la parte física	Separación de los ambientes de desarrollo, ensayo y operación. Se deben separar los ambientes de desarrollo, ensayo y operativos, para reducir los riesgos de acceso o cambios no autorizados al ambiente operacional.	Dirección, área de sistemas	Dirección, área de sistemas	30

Cuadro 6. Continuación

Vulnerabilidad	Descripción vulnerabilidad	Consecuencia	Control	Responsable	Ejecutante	Probabilidad vs impacto
Seguridad de las operaciones.	Se evidencia de la implementación de firewall - antivirus	Virus - ejecución no autorizado de programas - intrusión a red interna	Controles contra códigos maliciosos. Se deben implementar controles de detección, de prevención y de recuperación, combinarlos con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	Área de sistemas	Área de sistemas	20
	No se evidencia un procedimiento establecido para copias - aunque se realiza la actividad en discos duros	Pérdida de información - daño de los dispositivos de almacenamiento por mal uso -	Copias de respaldo de la información. Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.	Área de sistemas	Área de sistemas	40
	No se evidencia procedimiento documental para el manejo de los registros de eventos - aunque se realiza esta actividad mensualmente	Posible inexactitud de seguridad de la información en el análisis de los eventos al no ser periódico	Registro de eventos. Se deben elaborar, conservar y revisar regularmente los registros de eventos acerca de actividades del usuario, excepcionales, fallas y eventos de seguridad de la información.	Área de sistemas	Área de sistemas	20
	No se evidencia algún proceso en la protección de la información.	Fuga de información	Protección de la información de registro. Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.	Área de sistemas	Área de sistemas	20

Cuadro 6. Continuación

Vulnerabilidad	Descripción vulnerabilidad	Consecuencia	Control	Responsable	Ejecutante	Probabilidad vs impacto
Seguridad de las operaciones	Se evidencia registro del administrador, pero del operador no hay registros de operaciones	Intrusión – pérdida de información	Registros del administrador y del operador. Las actividades del administrador y del operador del sistema se deben registrar y los registros se deben proteger y revisar con regularidad.	Área de sistemas	Área de sistemas	20
	No se evidencia un procedimiento para la sincronización relojes	Modificación de operaciones	Sincronización de relojes. Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.	Área de sistemas	Área de sistemas	20
	No se evidencia un procedimiento que bloqueo instalación de software	Manipulación del sistema desmedido	Instalación de software en sistemas operativos. Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	Área de sistemas	Área de sistemas	20
	No se evidencia el análisis de riesgos.	Desconocimiento de la situación actual - sabotaje - fuga de información.	Gestión de las vulnerabilidades técnicas. Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	Área de sistemas	Área de sistemas	40

Cuadro 6. Continuación

Vulnerabilidad	Descripción vulnerabilidad	Consecuencia	Control	Responsable	Ejecutante	Probabilidad vs impacto
Seguridad de las operaciones	No se evidencia la existencia de reglamento para la instalación de software.	Modificación en las operaciones.	Restricciones sobre la instalación de software. Se debe establecer e implementar el reglamento de instalación de software por parte de los usuarios.	Área de sistemas	Área de sistemas	40
	No se evidencia de la existencia de auditorías sobre el sistema de información.	No existe planificación, ni control del sistema.	Controles sobre auditorías de sistemas de información. Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	Área de sistemas	Área de sistemas	40
Seguridad de las comunicaciones.	Se evidencia que hay control sobre la red - falta documentar el proceso.	Sistemas y aplicaciones inseguras.	Controles de redes. Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	Área de sistemas	Área de sistemas	10
	No se evidencia ni está documentado que mecanismos de seguridad existen para los servicios de red	Fuga de información.	Seguridad de los servicios de red. Se deben identificar los mecanismos de seguridad y los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.	Área de sistemas	Área de sistemas	20

Cuadro 6. Continuación

Vulnerabilidad	Descripción vulnerabilidad	Consecuencia	Control	Responsable	Ejecutante	Probabilidad vs impacto
Seguridad de las comunicaciones	Se evidencia de la separación de usuarios al interior de la red	Clasificación de la información – reserva.	Separación en las redes. Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.	Área de sistemas	Área de sistemas	10
	No se evidencia ninguna política y procedimientos de transferencia de información.	Divulgación de información - intrusos en la transferencia	Políticas y procedimientos de transferencia de información. Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información, mediante el uso de todo tipo de instalaciones de comunicaciones.	Área de sistemas	Área de sistemas	20
	No se evidencia de la existencia de los acuerdos sobre transferencia de información.	Desconocimiento de legal	Acuerdos sobre transferencia de información. Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.	Área de sistemas	Área de sistemas	20
	No se evidencia mecanismos documentados que permitan la protección de los mensajes electrónicos.	Fuga de información - ingeniería social	Mensajes electrónicos. Se debe proteger apropiadamente la información incluida en los mensajes electrónicos.	Área de sistemas	Área de sistemas	30

Cuadro 6. Continuación

Vulnerabilidad	Descripción vulnerabilidad	Consecuencia	Control	Responsable	Ejecutante	Probabilidad vs impacto
Seguridad de las comunicaciones	No se evidencia en ningún momento la existencia de procedimientos que coadyuven a la formulación de acuerdos de confidencialidad.	Fuga de información	Acuerdos de confidencialidad o de no divulgación. Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.	Área de sistemas	Área de sistemas	40
Adquisición, desarrollo y mantenimiento de sistemas.	No se evidencia la elaboración de análisis previos que contemplen los requisitos mínimos de la seguridad de la información para la adquisición de tecnología.	Proyección a corto, mediano y largo plazo de la empresa sin seguridad de la información - Pérdida de información - intrusión	Análisis y especificación de requisitos de seguridad de la información. Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	Dirección, área de sistemas	Dirección, área de sistemas	60
	No se evidencia la aplicación de seguridad de servicios para la aplicación en redes públicas.	Intrusión - Pérdida de información.	Seguridad de servicios de las aplicaciones en redes públicas. La información involucrada en servicios de aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	Área de sistemas	Área de sistemas	60

Cuadro 6. Continuación

Vulnerabilidad	Descripción vulnerabilidad	Consecuencia	Control	Responsable	Ejecutante	Probabilidad vs impacto
Adquisición, desarrollo y mantenimiento de sistemas.	No se evidencia procedimiento para la protección de transacciones de servicios de aplicaciones	Mensajes no autorizados - fuga de información - sabotaje electrónico)	Protección de transacciones de servicios de aplicaciones. La información involucrada en las transacciones de servicios de aplicaciones se debe proteger para prevenir la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes. La divulgación no autorizada y la duplicación o reproducción de mensajes no autorizados.	Área de sistemas	Área de sistemas	60
	No se evidencia política de desarrollo seguro	Sabotaje - perjudica imagen empresarial - Pérdida de información	Política de desarrollo seguro. Se deben establecer y aplicar reglas para el desarrollo de software y de sistemas a los desarrollos dentro de la organización.	Área de Sistemas	Área de Sistemas	40
	No se evidencia un procedimiento para la realización de cambio de sistema	No existe control de cambios	Procedimiento de control de cambios en sistemas. Los cambios a los sistemas dentro del ciclo de vida de desarrollo de software y de sistemas a los desarrollos dentro de la organización.	Área de sistemas	Área de sistemas	5
	No se evidencia la aplicación de un proceso de seguridad que revise las aplicaciones luego de los cambios	Indisponibilidad del servicio - Pérdida de información	Revisión técnica de aplicaciones después de cambios en la plataforma de operaciones. Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y poner a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad organizacionales.	Área de sistemas	Área de sistemas	30

Cuadro 6. Continuación

Vulnerabilidad	Descripción vulnerabilidad	Consecuencia	Control	Responsable	Ejecutante	Probabilidad vs impacto
Adquisición, desarrollo y mantenimiento de sistemas	No se evidencian restricciones para los cambios de su	Modificación de su ilimitado - alteración de las operaciones	Restricciones sobre los cambios de paquetes de software. Se deben desalentar las modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	Área de sistemas	Área de sistemas	20
	No se evidencia de la construcción de principios de sistemas seguros	Mal uso de las herramientas - fuga de información	Principios de construcción de sistemas de seguros. Se deben establecer, documentar y mantener principios para la organización de sistemas seguros, y aplicarlos a cualquier trabajo de implementación de sistemas de información.	Área de sistemas	Área de sistemas	20
	No se evidencia ni está documentado, la generación desarrollo seguro en la entidad	Fuga de información	Ambiente de desarrollo seguro. Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.	Área de sistemas	Área de sistemas	20
	Se evidencia supervisión de actividades de desarrollo por fuera de la entidad	Divulgación de la información confidencial - acceso no autorizado - deterioro imagen empresarial	Desarrollo contratado externamente. La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas subcontratados.	Área de sistemas	Área de sistemas	20

Cuadro 6. Continuación

Vulnerabilidad	Descripción vulnerabilidad	Consecuencia	Control	Responsable	Ejecutante	Probabilidad vs impacto
Adquisición, desarrollo y mantenimiento de sistemas	No se evidencian pruebas de seguridad para la implementación de actividades de desarrollo subcontratadas	Falla en el servicio -	Pruebas de seguridad de sistemas. Durante el desarrollo se deben llevar a cabo ensayos de funcionalidad de la seguridad.	Área de sistemas	Área de sistemas	20
	No se evidencia proceso para las pruebas de aceptación de sistemas	No hay un record de las pruebas de aceptación para consultas posteriores de implementación	Pruebas de aceptación de sistemas. Para los sistemas de información nuevos, actualizaciones y nuevas versiones se deben establecer programas de ensayo y criterios relacionados.	Área de sistemas	Área de sistemas	20
	No se evidencia protección de datos de ensayo	No hay seguimiento de las pruebas que se deben realizar	Protección de datos de ensayo. Los datos de ensayo se deben seleccionar, proteger y controlar cuidadosamente.	Área de sistemas	Área de sistemas	30
Relaciones con los proveedores	No se evidencia el establecimiento de la política de seguridad de la información con los proveedores	Sabotaje - perjudica imagen empresarial - Pérdida de información	Política de seguridad de la información para las relaciones con proveedores. Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con estos y se deben documentar.	Área de sistemas	Área de sistemas	60

Cuadro 6. Continuación

Vulnerabilidad	Descripción vulnerabilidad	Consecuencia	Control	Responsable	Ejecutante	Probabilidad vs impacto
Relaciones con los proveedores	No se evidencia acuerdos de seguridad de la información con los proveedores	Sabotaje - perjudica imagen empresarial - Pérdida de información	Tratamiento de la seguridad dentro de los acuerdos con proveedores. Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que puedan tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de ti para la información de la organización.	Área de sistemas	Área de sistemas	60
	No se evidencia la existencia de cadena de suministro de tecnología de información y comunicación	Sabotaje - perjudica imagen empresarial - Pérdida de información	Cadena de suministro de tecnología de información y comunicación. Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.	Área de sistemas	Área de sistemas	60
	No se evidencia un procedimiento para auditar los servicios de los proveedores	Acceso no autorizado - modificación en las operaciones	Seguimiento y revisión de los servicios de los proveedores. Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	Área de sistemas	Área de sistemas	60

Cuadro 6. Continuación

Vulnerabilidad	Descripción vulnerabilidad	Consecuencia	Control	Responsable	Ejecutante	Probabilidad vs impacto
Relaciones con los proveedores	No se evidencia la gestión de cambios a los servicios de los proveedores	Por la falta de planeamiento metodológico se puede incurrir en fallas constantes	Gestión de cambios a los servicios de los proveedores. Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados y la reevaluación de los riesgos.	Área de sistemas	Área de sistemas	60
Gestión de incidentes de seguridad de la información.	No se evidencia procedimientos de gestión de incidentes	Desconocimiento de los riesgos e incidentes	Responsabilidades y procedimientos. Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	Área de sistemas	Área de sistemas	60
	No se evidencia que los eventos de seguridad que se presentan sean informados	Desconocimiento de los eventos de seguridad	Informe de eventos de seguridad de la información. Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados tan pronto como sea posible.	Área de Sistemas	Área de Sistemas	60

Cuadro 6. Continuación

Vulnerabilidad	Descripción vulnerabilidad	Consecuencia	Control	Responsable	Ejecutante	Probabilidad vs impacto
Gestión de incidentes de seguridad de la información.	No se evidencia la existencia de un proceso de retroalimentación de las debilidades de seguridad de la información	No hay avance por falta de comunicación y divulgación de las debilidades encontradas en la seguridad de la información	Informe de debilidades de seguridad de la información. Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que se observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	Área de sistemas	Área de sistemas	30
	No se evidencia evaluación de eventos de la seguridad de la información	Desconocimiento de los eventos que se presentan en ave	Evaluación de eventos de seguridad de la información y decisiones sobre ellos. Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.	Área de sistemas	Área de sistemas	30
	No existe evidencia de respuestas de incidentes de la seguridad de la información	Acceso no autorizado - modificación en las operaciones	Respuesta a incidentes de seguridad de la información. Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	Área de sistemas	Área de sistemas	30
	No se aplica el conocimiento de los incidentes para mejorar la seguridad	Desconocimiento del propio sistema de seguridad y avances del mismo	Aprendizaje obtenido de los incidentes de seguridad de la información. El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros.	Área de sistemas	Área de sistemas	20

Cuadro 6. Continuación

Vulnerabilidad	Descripción vulnerabilidad	Consecuencia	Control	Responsable	Ejecutante	Probabilidad vs impacto
Gestión de incidentes de seguridad de la información.	No existe un procedimiento que salvaguarde la evidencia.	Pérdida de información valiosa para el tema de los incidentes encontrados	Recolección de evidencia. La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	Área de sistemas	Área de sistemas	20
Continuidad de negocio.	No se evidencia planificación de la continuidad de la seguridad de la información.	El avance no es tangible	Planificación de la continuidad de la seguridad de la información. La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastres.	Área de sistemas	Área de sistemas	30
	No se evidencia de procedimientos ni controles que aseguren la información.	Des aseguramiento de la información en todos los niveles	Implementación de la continuidad de la seguridad de la información. La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	Área de sistemas	Área de sistemas	30
	No se evidencia que exista una verificación de los controles de la seguridad de la información.	Estancamiento de la entidad en la seguridad de la información	Verificación, revisión y evaluación de la continuidad de la seguridad de la información. La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información implementados con el fin de asegurar que los válidos y eficaces durante situaciones adversas.	Área de sistemas	Área de sistemas	30
	No se evidencia la existencia de mecanismos que aseguren la disponibilidad del procesamiento de información.	Negación de servicio	Disponibilidad de instalaciones de procesamiento de información. Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	Área de sistemas	Área de sistemas	60

Cuadro 6. Continuación

Vulnerabilidad	Descripción vulnerabilidad	Consecuencia	Control	Responsable	Ejecutante	Probabilidad vs impacto
Cumplimiento	No se evidencia documentación legal	Desconocimiento de las responsabilidades legales - para la entidad y para los empleados	Identificación de los requisitos de legislación y contractuales aplicables. Se deben identificar, documentar y mantener actualizados explícitamente todos los requisitos legislativos estatutarios, de reglamentación y contractuales pertinentes, y el enfoque de la organización para cada sistema de información y para la organización.	Área sistemas	Área sistemas	60
	No se evidencia un proceso que establezca manejo pertinente para el uso de productos de software licenciados	Incumplimiento a la ley	Derechos de propiedad intelectual. Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software licenciados.	Área sistemas	Área sistemas	60
	No se evidencia un procedimiento para la protección de registros	Modificación de información - acceso no autorizados - Pérdida de información	Protección de registros. Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	Área sistemas	Área sistemas	60
	No se evidencia que se asegure la privacidad y protección de la información	Alteración de la integridad de la información	Privacidad y protección de la información identificable personalmente. Se deben asegurar la privacidad y la protección de la información identificable personalmente, como se exige en la legislación y la reglamentación pertinentes, cuando sea aplicable.	Área sistemas	Área sistemas	60

Cuadro 6. Continuación

Vulnerabilidad	Descripción vulnerabilidad	Consecuencia	Control	Responsable	Ejecutante	Probabilidad vs impacto
Cumplimiento	No se evidencia de la aplicación de mecanismo que encripte la información de la entidad bajo los parámetros establecidos	Divulgación de información - imagen empresarial - Pérdida de información	Reglamentación de controles criptográficos. Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos.	Área sistemas	Área sistemas	30
Cumplimiento	No se evidencia la revisión independiente de la seguridad cuando ocurra cambios significativos	Des aseguramiento de la información	Revisión independiente de la seguridad de la información. El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.	Área sistemas	Área sistemas	30
	No se evidencia el cumplimiento y seguimiento de las políticas y normas de seguridad	Des aseguramiento de la información	Cumplimiento con las políticas y normas de seguridad. Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas y cualquier otro requisito de seguridad.	Área sistemas	Área sistemas	30
	No se evidencia que se realice una revisión del cumplimiento técnico	Desatención del incumplimiento técnico - fallas técnicas constantes	Revisión del cumplimiento técnico. Los sistemas de información se deben revisar con regularidad para determinar el cumplimiento con las políticas y normas de seguridad de la información.	Área sistemas	Área sistemas	30

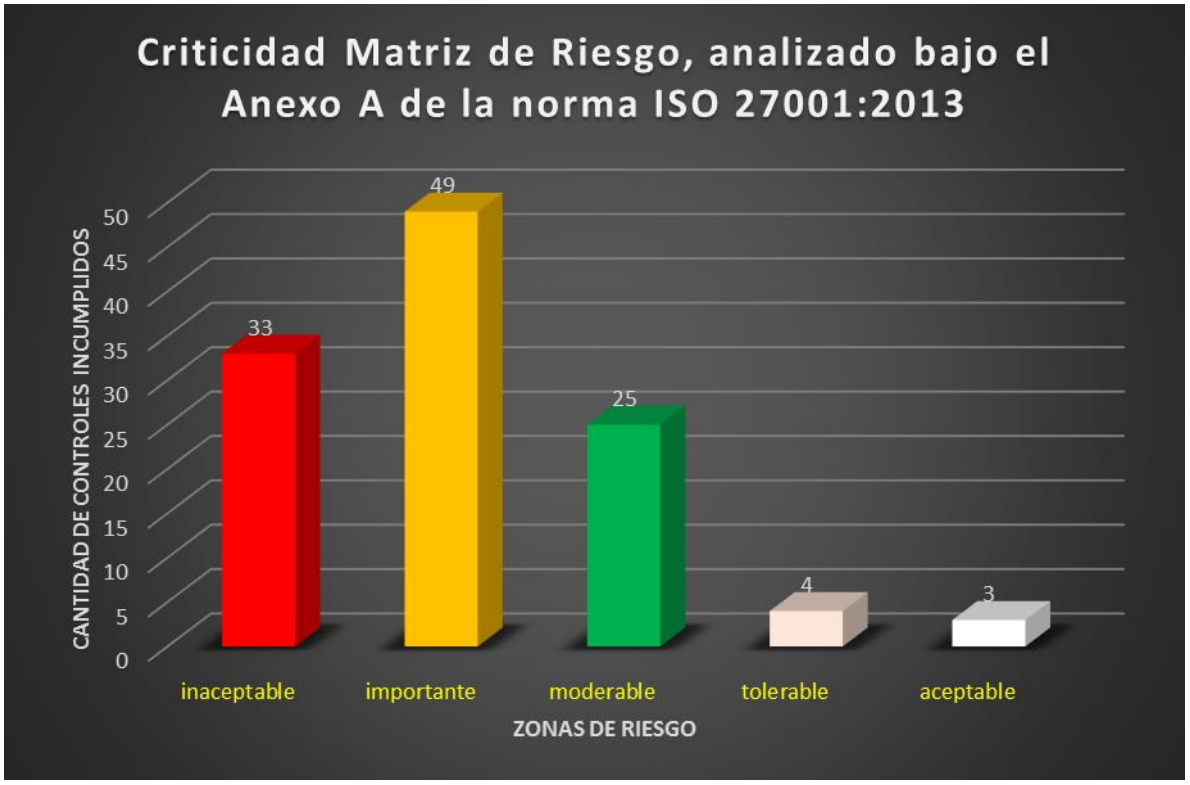
Fuente: Autores.

A continuación se encuentra representado en graficas los estados de incumplimiento de riesgo basándose en la norma ISO 27001:2013. Establecidos en las zonas del riesgo de la empresa y de la información obtenida en las encuestas que se realizaron al personal de la empresa.

8.1.3 Consolidado Objetivos de Control y Cantidad de Controles Norma ISO 27001-2013

De acuerdo con la Figura 23, se evidencia la criticidad de las zonas de riesgo establecidas bajo la matriz de riesgo y la cantidad de controles incumplidos. en cuanto al análisis del Anexo A de la norma ISO 27001:2013; el resultado del instrumento de la encuestas realizadas, confirman la información obtenida de este planeamiento.

Figura 23. Incumplimiento Objetivos de control



Fuente: Autores.

8.2 RESULTADO DE INCUMPLIMIENTO DE LA NORMA ISO 27001:2013

Con el fin de realizar una propuesta coherente en cuanto al incumplimiento de la normatividad específicamente de la ISO 27001:2013, se realizó a la Empresa , en compañía del Ingeniero de Sistemas, quien evaluó y aprobó los resultados obtenidos.

Para obtener un resultado porcentual que permita observar mejor el incumplimiento se tomó la cantidad de los controles por cada uno de los numerales como el 100%, posterior a esto, se realizó una ecuación regla de tres que permitiera identificar cual sería el porcentaje de incumplimiento de la norma ISO27001:2013, como lo indica el Cuadro 7. Resultado del Anexo A de la norma

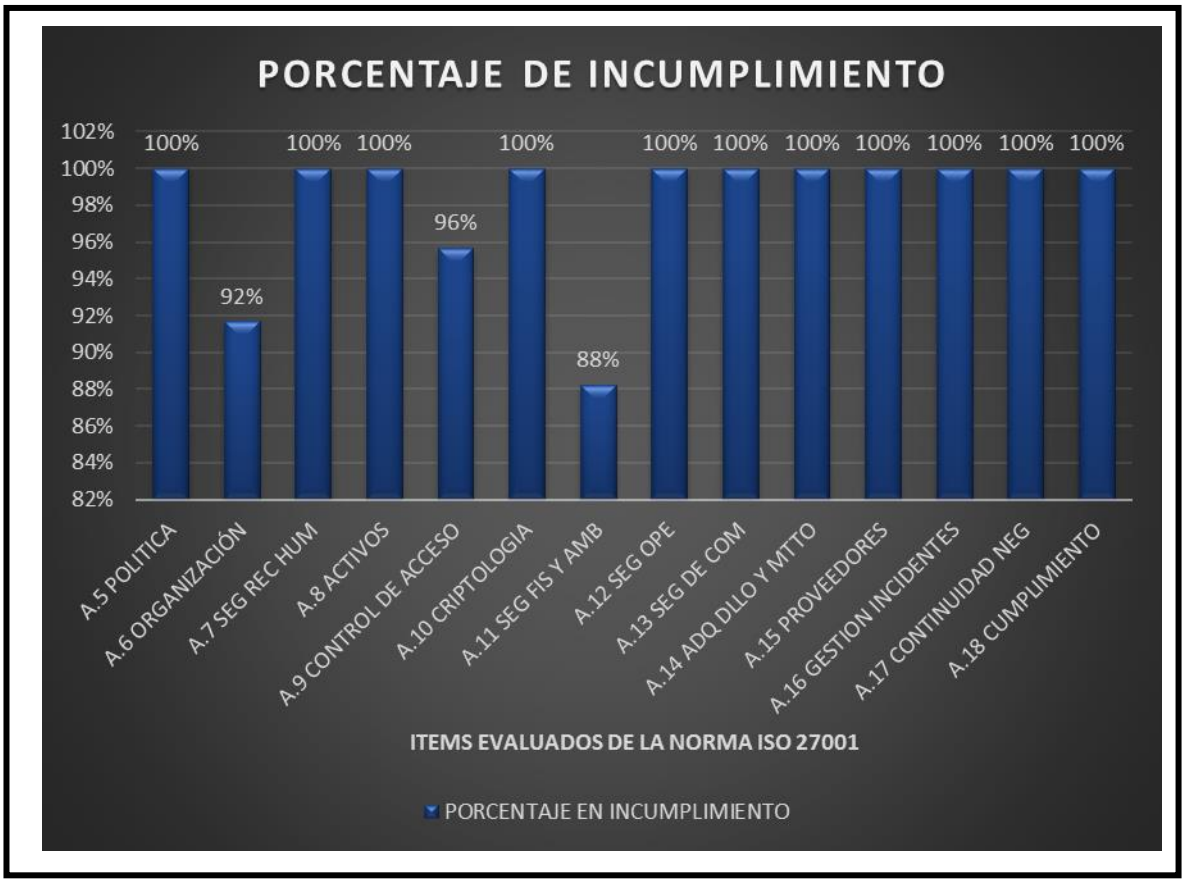
Cuadro 7. Resultados de la norma ISO 27001:2013

Numeral	Porcentaje en incumplimiento	Porcentaje en cumplimiento
A.5 Política	100%	0%
A.6 Organización	92%	8%
A.7 Seguridad Recursos Humanos	100%	0%
A.8 Activos	100%	0%
A.9 Control de Acceso	96%	4%
A.10 Criptografía	100%	0%
A.11 Seguridad Física y Ambiental	88%	12%
A.12 Seguridad Operaciones	100%	0%
A.13 Seguridad de Comunicaciones	100%	0%
A.14.Adquisición Desarrollo y Mantenimiento	100%	0%
A.15 Proveedores	100%	0%
A.16 Gestión Incidentes	100%	0%
A.17 Continuidad Negocio	100%	0%
A.18 Cumplimiento	100%	0%

Fuente: Autores.

En el Cuadro 7, se observa que actualmente incumple once (11) de los numerales de la norma ISO 27001:2013 con un porcentaje del 100% de 14 numerales, así mismo, refleja que tres numerales presentan algún tipo de actividad interna Aunque el porcentaje de cumplimiento es mínimo, es un valor importante para este estudio, toda vez que representa la preocupación y los primeros pasos en cuanto al tema de seguridad de la información.

Figura 24. Porcentaje de incumplimiento



Fuente: Autores.

Teniendo en cuenta la Figura 28, refleja gráficamente el porcentaje de incumplimiento en cuanto a la norma ISO 27001:2013.

Figura 25. Indicadores de cumplimiento

Fuente: Autores.

De acuerdo con la Figura 29, refleja el resultado que permite identificar que no cuenta con políticas de seguridad establecidas que permita salvaguardar los activos (información) de la manera adecuada. La mayoría de los numerales se encuentran con un porcentaje de incumplimiento alto, lo que permite identificar que posiblemente desconoce el objetivo y la finalidad de la norma ISO 27001:2013.

9. VERIFICACIÓN Y APLICACIÓN DE LA NORMA ISO 27001:2013

Con el fin de realizar una propuesta adecuada se realizó inicialmente una visita de campo en sitio, que permitiera reflejar las falencias que tiene actualmente en seguridad de la información. Teniendo en cuenta lo anterior, se da inició a la evaluación de los numerales de la norma y subitem de la ISO 27001:2013. Así mismo, y con el propósito de mantener un orden de los hallazgos encontrados por numeral, se designó un número consecutivo para lograr una mejor coherencia en los resultados.

9.1 HALLAZGO 01 POLÍTICA PARA LA SEGURIDAD DE LA INFORMACIÓN

Fecha: 03 de agosto de 2015.

Numeral: políticas para la seguridad de la información.

Subitem:

Orientación de la dirección para la Gestión de la Seguridad de la Información.
Revisión de las Políticas para seguridad de la información. Las Políticas para Seguridad de la Información se deben revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su idoneidad, adecuación y eficacia continúas.

Criterio: Verificar si se encuentran implementadas Políticas de Seguridad, las cuales deberán estar aprobadas, hayan sido publicadas y difundidas para todo el personal.

Causa: Desconocimiento de la importancia de la seguridad de la información.

Efecto:

- Información no segura.
- Incumplimiento a los parámetros establecidos internos y externos que el sistema proporciona.
- Falta de control del sistema de información.

Conclusión: No cumple con la política de seguridad establecida en la norma ISO 27001; lo que indica en primera medida el desconocimiento de la Alta Gerencia de la importancia que tiene la seguridad de la información en la entidad.

Recomendación: Orientar la construcción de la política de seguridad clara, y con unos objetivos que permitan asegurar la continuidad del negocio.

El área de sistemas debe propender por colocar en conocimiento de las ventajas y desventajas de implementar un sistema de seguridad de la información.

9.2 HALLAZGO 02 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Fecha: 03 de agosto de 2015.

Numeral: Organización de la Seguridad de la Información.

Subitem:
- Organización Interna.
- Dispositivos Móviles y Teletrabajo.

Criterio: Verificar la existencia si existen políticas de seguridad adecuadas para el manejo de la organización interna y dispositivos móviles y teletrabajo.

Causa:

- No se encuentran definidos ni documentados los roles y responsabilidades del personal.
- No se evidencia contacto con autoridades pertinentes.
- Se evidencian la existencia de mínimas políticas de seguridad en cuanto al acceso de dispositivos móviles.
- No se evidencia una política que contenga medidas de seguridad para salvaguardar la información, la cual es manipulada por todo el personal administrativo y operativo.
- Se evidencia que se realizan actividades propias del área de sistemas en áreas ajenas a ella, pero no se encuentran documentadas ni registradas.

Efecto:

- Negligencia por parte del personal, el cual puede ser calculado en pérdidas.
- Pérdida de información.

- Desconocimiento de temas asociados al tema de seguridad-no existe un medio para retroalimentar fallos del sistema por el personal.

Conclusión: No se evidencia el establecimiento de políticas de seguridad para la organización interna ni para el uso de dispositivos móviles y teletrabajo

Recomendación: Se sugiere establecer políticas de seguridad para el personal que interviene en el sistema, que garanticen la corresponsabilidad del personal y las Directivas, así como las restricciones pertinentes para los dispositivos móviles.

9.3 HALLAZGO 03 SEGURIDAD DE LOS RECURSOS

Fecha: 03 de agosto de 2015

Numeral: Seguridad de los Recursos Humanos.

Subitem:

- Durante la ejecución del empleo.
- Terminación y cambio de empleo.

Criterio: Verificar la implementación de una política de seguridad para el personal que trabaja.

Causa:

- No se realiza el proceso de estudio para el personal que labora
- No evidencia la aplicación de la seguridad para los empleados ni los contratistas.
-
- Falta de capacitación para el personal que hace parte de los procesos en
- No se evidencia de la existencia de un proceso que establezca acciones formales en el caso de violentar algunos de los sistemas de seguridad.
- No se evidencia la existencia proceso y/o métodos para informar la terminación o cambio de responsabilidad de empleo.

Efecto:

- Extracción de información de acuerdo al nivel de clasificación de la información.
- Desconocimiento - posible fuga de información.
- Perjuicio para la imagen empresarial.
- Desconocimiento de la ley.

- No hay compromiso ni responsabilidad del empleado y del empleador.

Conclusión: Se puede concluir que no existe una política de seguridad para el área de recursos humanos, esta área es parte fundamental para generar controles, que garanticen que el personal que ingresa es idóneo para el cargo que está siendo designado o por el contrario si ha culminado su labor.

Recomendación: Generar una política de seguridad para esta área, considerando que el recurso humano es una prioridad y por lo tanto debe cumplir con los requisitos establecidos en la política y por ende en la entidad; de igual manera debe ser clara y debe ser conocida por las dos partes.

9.4 HALLAZGO 04 GESTIÓN DE ACTIVOS

Fecha: 03 de agosto de 2015

Numeral: Gestión de Activos}

Subitem:

- Responsabilidad por los Activos.
- Clasificación de la Información.
- Manejo de medios de soporte.

Criterio: Verificación de la existencia de una política de seguridad en cuanto a los activos, clasificación de la información y para el manejo de medios de soporte.

Causa:

- No se evidencia la existencia de un inventario de activos.
- No se evidencia proceso de verificación de activos en calidad de préstamos.
- No se evidencia la existencias de mecanismos quede a conocer cuál es la manera adecuada de manipular los activos.
- No se evidencia la existencia de un proceso de devolución de activos para los empleados.
- No se evidencia un proceso que clasifique la información.
- No se evidencia un proceso que etiquetado de la información.
- Se evidencia que existe un proceso para el manejo de los activos.
- No se evidencia un tratamiento para los medios de soporte removibles.
- No se evidencia de un proceso para la transferencia de medios de soporte físicos.

Efecto:

- Información no confiable de los activos.
- Desorganización de las actividades del área de sistemas para realizar mantenimiento sin programación.
- Desconocimiento de los equipos que no son propios.
- Mal manejo de los activos.
- Deterioro de los activos.
- Pérdida de tiempo en las labores propias por falta de un cronograma de trabajo.
- Aumento de costos.
- Aumento en la desviación de los activos.
- Aumento de las necesidades tecnológicas.
- pérdida de información.
- Divulgación de información por personal no autorizado.
- Control con los activos.
- Fuga de información - pérdida de datos.
- Falta de control de los activos.
- Fuga de información - uso mal intencionado.

Conclusión: Se evidencia que no existe política de seguridad para los activos. La información no es confiable, dado que la inexistencia de un proceso documentado.

Recomendación: Diseñar una política de seguridad, que garantice que estos procesos contengan información verídica y real de los activos.

9.5 HALLAZGO 05 CONTROL DE ACCESO

Fecha: 03 de agosto de 2015

Numeral: Control de acceso.
Subitem:

- Requisitos del Negocio para Control de Acceso.
- Gestión de Acceso de Usuarios.
- Responsabilidades de los usuarios.
- Control de Acceso a Sistemas y Aplicaciones.

Criterio: Verificar si la empresa tiene un procedimiento detallado y documentado que controle el acceso en todas las áreas que requieren del mismo.

Causa:

- No existe política control de acceso.
- No se evidencia control de acceso a la red y a los servicios.
- No se evidencia control del registro y cancelación de usuarios.

- No se evidencia un mecanismo para el suministro de acceso a los usuarios.
- No se evidencia la existencia de algún proceso de gestión formal para la autenticación secreta de usuarios.
- No se evidencia la existencia de revisiones periódicas de acceso de los usuarios.
- Acceso de dispositivos móviles sin restricción.
- Desconocimiento de información secreta y el cuidado que deben tener los empleados.
- No se evidencia restricción de acceso a la información.
- No se evidencia la existencia de un procedimiento de conexión segura.
- No se evidencia un procedimiento de gestión de contraseñas.
- No se evidencia el control sobre programas utilitarios.
- No se evidencia un procedimiento para el control de acceso al código fuente.

Efecto:

- Desconocimiento del personal de una política de control acceso.
- Ingreso personal no autorizado - manipulación inadecuada de la información y los servicios.
- Fuga de información.
- Uso inadecuado de la información.
- La no existencia del procedimiento permite accesos no autorizados ni el establecimiento de responsabilidades.
- Accesos sin control.
- Acceso sin control, para el personal que es ajeno a la entidad mala manipulación y divulgación de la información.
- Acceso no autorizado - modificación en las operaciones.
- No se aplica contraseñas de acuerdo al procedimiento.
- Anulación del sistema - denegación de servicio.
- Modificación de información - accesos no autorizados.

Conclusión: No se evidencia una política de seguridad para estos efectos toda vez que garantice que estos procesos se realicen de la manera adecuada, a la vez no hay nada documentando.

Recomendación: Diseñar una política de seguridad, que permita cumplir con todos los requisitos.

9.6 HALLAZGO 06 CRIPTOGRAFÍA

Fecha: 03 de agosto de 2015

Numeral: Criptografía.

Subitem: Controles Criptográficos.

Criterio: Verificar si existe una política de criptografía.
Causa:

- No se evidencia la existencia de una política que aplique los controles criptográficos.
- No se evidencia la existencia de un procedimiento de gestión de claves.

Efecto:

- Divulgación de la información.
- Alteración de los principios de la seguridad de la información.

Conclusión: no cuenta con una política de seguridad que apunte a proteger la información que se envía interna y externa.

Recomendación: Diseñar una política capaz de controlar y proteger la información que se envía y se reciben por los diferentes canales de transmisión.

9.7 HALLAZGO 07 SEGURIDAD FÍSICA Y AMBIENTAL

Fecha: 03 de agosto de 2015

Numeral: Seguridad física y ambiental.

Subitem:

- Áreas Seguras.
- Equipos.

Criterio: Verificar que exista un procedimiento que permita asegurar la parte física y ambiental.

Causa

- No se evidencia la delimitación de perímetro de seguridad.
- La oficina de sistemas no cumple con los controles físicos de entrada.
- La oficina de sistemas de ave, es compartida con otro usuario.
- No se evidencia la existencia de un procedimiento contra las amenazas ambientales.
- No se evidencia que se coloque en práctica el tema de trabajo en áreas seguras.

- Manejo inadecuado de contraseñas (inseguras, no cambian, compartidas).
- Falta de inducción, capacitación y sensibilización de los riesgos informáticos.
- Se evidencia la existencia de planta eléctrica para los equipos ups.
- No se evidencia la existencia del procedimiento de seguridad de cableado de datos.
- No se evidencia la existencia de un cronograma de mantenimiento a los activos.
- No se evidencia procedimiento para el trámite de retiro de activos.
- No se evidencia procedimiento para el trámite de seguridad para los activos fuera de la empresa.
- No se evidencia de la existencia de un procedimiento que trate sobre los - desechos electrónicos y/o reutilización de equipos.
- Falta de inducción, capacitación y sensibilización de los riesgos informáticos.
- No se evidencia procedimiento para tratar la política de escritorio limpio y pantalla limpia - falta capacitación - desconocimiento de la norma.

Efecto:

- El espacio que existe para el almacenamiento de información.
- Fuga de información - alteración en las operaciones - acceso no autorizado – vandalismo.
- Allanamiento ilegal.
- Pérdida de información - desestabilización del sistema.
- Pérdida de información - sabotaje (ataque físico y/o electrónico).
- Pérdida y/o modificación de información
- Medio que subsana cualquier falla de corriente
- Red cableada expuesta para el acceso no autorizado.
- Se permite la disponibilidad de la información - desconocimiento de necesidades tecnológicas.
- Falta de control en los activos.
- Divulgación de información - tramite inadecuado de la información - contaminación ambiental.
- Perjuicio para la imagen empresarial.
- Información vulnerable.

Conclusión: Se evidencia que no existe una política de seguridad física y ambiental, que garantice todos los requisitos de seguridad de la información.

Recomendación: Diseñar una política de seguridad que permita proteger el área de seguridad física y ambiental; toda vez, que si estos parámetros se cumplen, se minimizan de manera significativa los riesgos encontrados.

9.8 HALLAZGO 08 SEGURIDAD DE LAS OPERACIONES

Fecha: 03 de agosto de 2015

Numeral: Seguridad de las Operaciones.

Subitem: La oficina de sistemas de ave, es compartida con otro usuario.

Criterio: Verificar si asegura las operaciones internas y externas.

Causa:

- No se evidencia la delimitación de perímetro de seguridad.
- La oficina de sistemas no cumple con los controles físicos de entrada.
- La oficina de sistemas de ave, es compartida con otro usuario.
- No se evidencia la existencia de un procedimiento contra las amenazas ambientales.
- No se evidencia que se coloque en práctica el tema de trabajo en áreas seguras.
- Manejo inadecuado de contraseñas (inseguras, no cambian, compartidas)
- Falta de inducción, capacitación y sensibilización de los riesgos informáticos.
- Se evidencia la existencia de planta eléctrica para los equipos ups.
- No se evidencia la existencia del procedimiento de seguridad de cableado de datos.
- No se evidencia la existencia de un cronograma de mantenimiento a los activos.
- No se evidencia procedimiento para el trámite de retiro de activos.
- No se evidencia procedimiento para el trámite de seguridad para los activos.
- No se evidencia de la existencia de un procedimiento que trate sobre los desechos electrónicos y/o reutilización de equipos.
- Falta de inducción, capacitación y sensibilización de los riesgos informáticos.
- No se evidencia procedimiento para tratar la política de escritorio limpio y pantalla limpia - falta capacitación - desconocimiento de la norma.

Efecto:

- Desconocimiento en cuanto a la forma de seguir los procedimientos.
- Por la falta de planeamiento metodológico se puede incurrir en fallas constantes.
- No se evidencia la verifica periódica para proyecciones requeridas al sistema.
- Aumento significativo de acceso no autorizado para la parte física.
- Virus - ejecución no autorizada de programas - intrusión a red interna.
- Pérdida de información - daño de los dispositivos de almacenamiento por mal uso.
- Posible inexactitud de seguridad de la información en el análisis de los eventos al no ser periódico.

- Fuga de información.
- Modificación de operaciones.
- Manipulación del sistema desmedido.
- Desconocimiento de la situación actual - sabotaje - fuga de información
- Modificación en las operaciones.

Conclusión: no tiene contemplado la aplicación de una política de seguridad para las Operaciones.

Recomendación: Diseñar una política de seguridad que permita evaluar y controlar la seguridad de las operaciones, internas y externas.

9.9 HALLAZGO 09 SEGURIDAD DE LAS COMUNICACIONES

Fecha: 03 de agosto de 2015

Numeral: Seguridad de las comunicaciones.

Subitem: Transferencia de información.

Criterio: Verificar la existencia de una política de seguridad para las comunicaciones.

Causa:

- Se evidencia que hay control sobre la red - falta documentar los procesos.
- No se evidencia ni está documentado que mecanismos de seguridad existen para los servicios de red.
- No se evidencia de la separación de usuarios al interior de la red.
- No se evidencia ninguna política y procedimientos de transferencia de información.
- No se evidencia de la existencia de los acuerdos sobre transferencia de información.
- No se evidencia mecanismos documentados que permitan la protección de los mensajes electrónicos.
- No se evidencia en ningún momento la existencia de procedimientos que coadyuven a la formulación de acuerdos de confidencialidad.

Efecto:

- Sistemas y aplicaciones inseguras.
- Fuga de información.

- Clasificación de la información – reserva.
- Divulgación de información - intrusos en la transferencia.
- Desconocimiento del marco legal.
- Ingeniería social.

Conclusión: Se concluye que no se encuentra diseñada una política de seguridad para las Comunicaciones.

Recomendación: Diseñar una política de seguridad, que garantice el medio por el cual se transporta la información.

9.10 HALLAZGO 10 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

Fecha: 03 de agosto de 2015

Numeral: Adquisición, desarrollo y mantenimiento de sistemas.

Subitem:

- **Requisitos de seguridad de los sistemas de información.**

- Seguridad en los procesos de desarrollo y de soporte.
- Objetivo. Asegurar la protección de los datos usados para ensayos.
- **Criterio:** verificar la existencia de una política de seguridad para la Adquisición, desarrollo y mantenimiento de sistemas.

Causa:

- No se evidencia la elaboración de análisis previos que contemplen los requisitos mínimos de la seguridad de la información para la adquisición de tecnología.
- No se evidencia la aplicación de seguridad de servicios para la aplicación en redes públicas.
- No se evidencia procedimiento para la protección de transacciones de servicios de aplicaciones.
- No se evidencia política de desarrollo seguro.
- No se evidencia un procedimiento para la realización de cambio de sistema
- No se evidencia la aplicación de un proceso de seguridad que revise las aplicaciones luego de los cambios.
- No se evidencian restricciones para los cambios de software.
- No se evidencia de la construcción de principios de sistemas seguros.
- No se evidencia ni está documentado, la generación desarrollo seguro en la entidad.
- Se evidencia supervisión de actividades de desarrollo por fuera de la entidad.

- No se evidencian pruebas de seguridad para la implementación de actividades de desarrollo subcontratadas.
- No se evidencia proceso para las pruebas de aceptación de sistemas
- No se evidencia protección de datos de ensayo.

Efecto:

- Proyección a corto, mediano y largo plazo de la empresa sin seguridad de la información - Pérdida de información – intrusión.
- Intrusión.
- Mensajes no autorizados - fuga de información - sabotaje electrónico).
- Sabotaje - perjudica imagen empresarial.
- Indisponibilidad del servicio - Pérdida de información.
- Modificación de software ilimitado - alteración de las operaciones.
- Mal uso de las herramientas.
- Fuga de información.
- Divulgación de la información confidencial - acceso no autorizado - deterioro imagen empresarial.
- Falla en el servicio.
- No hay un record de las pruebas de aceptación para consultas posteriores de implementación.
- No hay seguimiento de las pruebas que se deben realizar.

Conclusión: se concluye que en no se encuentra diseñada una política de seguridad para los procesos de adquisición, desarrollo y mantenimiento de sistemas.

Recomendación: diseñar una política de seguridad, que garantice la adquisición de equipos, desarrollo y mantenimiento de sistemas.

9.11 HALLAZGO 11 RELACIONES CON LOS PROVEEDORES

Fecha: 03 de agosto de 2015

Numeral: Relaciones con los proveedores.

Subitem:

- Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.
- Gestión de la prestación de servicios de proveedores.

Criterio: Verificar la existencia de una política de seguridad que asegure las relaciones con los proveedores.

Causa:

- No se evidencia el establecimiento de la política de seguridad de la información con los proveedores.
- No se evidencia acuerdos de seguridad de la información con los proveedores.
- No se evidencia la existencia de cadena de suministro de tecnología de información y comunicación.
- No se evidencia un procedimiento para auditar los servicios de los proveedores.
- No se evidencia la gestión de cambios a los servicios de los proveedores.

Efecto:

- Sabotaje - perjudica imagen empresarial -pérdida de información.
- Acceso no autorizado - modificación en las operaciones.
- Por la falta de planeamiento metodológico se puede incurrir en fallas constantes.

Conclusión: Se concluye que no se encuentra diseñada una política de seguridad en cuanto a la relación con los proveedores.

Recomendación: Diseñar una política de seguridad, que garantice las relaciones con los proveedores, sin exponer ninguna de las dos partes.

9.12 HALLAZGO 12 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Fecha: 03 de agosto de 2015

Numeral: Gestión de incidentes de seguridad de la información.

Subitem: Gestión de incidentes y mejoras en la seguridad de la información.

Criterio: Verificar la existencia de una política de seguridad para las comunicaciones.

Causa:

- No se evidencia procedimientos de gestión de incidentes.
- No se evidencia que los eventos de seguridad que se presentan sean informados.
- No se evidencia la existencia de un proceso de retroalimentación de las debilidades de seguridad de la información.
- No se evidencia evaluación de eventos de la seguridad de la información.
- No existe evidencia de respuestas de incidentes de la seguridad de la información.
- No se aplica el conocimiento de los incidentes para mejorar la seguridad.
- No existe un procedimiento que salvaguarde la evidencia

Efecto:

- Desconocimiento de los riesgos e incidentes.
- Desconocimiento de los eventos de seguridad.
- No hay avance por falta de comunicación y divulgación de las debilidades encontradas en la seguridad de la información.
- Desconocimiento de los eventos que se presentan en Ave Colombia S.A.S.
- Acceso no autorizado - modificación en las operaciones.
- Desconocimiento del propio sistema de seguridad y avances del mismo.
- Pérdida de información valiosa para el tema de los incidentes encontrados.

Conclusión: Se concluye que, no se encuentra diseñada una política de seguridad que impacte gestión de incidentes y mejoras en la seguridad de la información.

Recomendación: Diseñar una política de seguridad, que garantice una gestión de incidentes y mejoras en la seguridad de la información.

9.13 HALLAZGO 03 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIO

Fecha: 03 de agosto de 2015

Numeral: Aspectos de seguridad de la información de la gestión de la continuidad de negocio.

Subitem:

- Continuidad de seguridad de la información.
- Redundancia.

Criterio: Verificar la existencia de una política de seguridad que asegure las la continuidad el negocio.

Causa:

- No se evidencia planificación de la continuidad de la seguridad de la información.
- No se evidencia de procedimientos ni controles que aseguren la información.
- No se evidencia que exista una verificación de los controles de la seguridad de la información.
- No se evidencia la existencia de mecanismos que aseguren la disponibilidad del procesamiento de información.

Efecto:

- El avance no es tangible.
- Des aseguramiento de la información en todos los niveles.
- Estancamiento de la entidad en la seguridad de la información
- Negación de servicio.

Conclusión: se concluye que no se encuentra diseñada una política que garantice la continuidad del negocio.

Recomendación: diseñar una política de seguridad, que garantice la continuidad del negocio.

9.14 HALLAZGO 14 CUMPLIMIENTO

Fecha: 03 de agosto de 2015

Numeral: Cumplimiento

Subitem:

- Cumplimiento de requisitos legales y contractuales.
- Revisiones de seguridad de la información.

Criterio: Verificar la existencia de una política de seguridad que asegure la revisión, protección, generación de reglamentos como parte del cumplimiento de la norma.

Causa:

- No se evidencia documentación legal.
- No se evidencia un proceso que establezca manejo pertinente para el uso de - productos de software licenciados.
- No se evidencia un procedimiento para la protección de registros.
- No se evidencia que se asegure la privacidad y protección de la información.
- No se evidencia de la aplicación de mecanismo de encriptación de información de la entidad bajo los parámetros establecidos.
- No se evidencia la revisión independiente de la seguridad cuando ocurran cambios significativos.
- No se evidencia el cumplimiento y seguimiento de las políticas y normas de seguridad.
- No se evidencia que se realice una revisión del cumplimiento técnico

Efecto:

- Desconocimiento de las responsabilidades legales - para la entidad y para los empleados
- Incumplimiento a la ley.
- Modificación de información - acceso no autorizado - pérdida de información
- Alteración de la integridad de la información.
- Divulgación de información - imagen empresarial - pérdida de información
- Des aseguramiento de la información
- Desatención del incumplimiento técnico - fallas técnicas constantes

Conclusión: Se concluye que no se encuentra diseñada una política de seguridad que permita cumplir a cabalidad la implantación de un sistema de seguridad de la información.
Recomendación: Diseñar una política de seguridad, el cumplimiento de la implementación, sin olvidar los principios de la seguridad.

10. CONCLUSIONES

Este análisis de seguridad permitió realizar una planificación de un sistema de gestión y seguridad de la información para el área de sistemas bajo la norma ISO 27001:2013.

Frente al cumplimiento de la norma, el Sistema de Seguridad se encuentra en la primera etapa de madurez, y los resultados que se evidenciaron en este trabajo, reflejan la situación actual por la falta de un seguimiento periódico.

Al elaborar el análisis de riesgo basado en la norma ISO 27001:2013 permitió identificar con mayor claridad las falencias que se encuentran en todos los niveles de la entidad, y que requieren ser tratados en el menor tiempo posible.

Podemos establecer que no cuenta con un mecanismo de comunicación eficiente, que permita divulgar oportunamente los objetivos, políticas de seguridad de la información y las expectativas que se tiene en cuanto a la planificación de un sistema de gestión de información basado en la norma ISO27001:2013.

De acuerdo a las encuestas y entrevistas realizadas se obtuvo información de gran interés que permitió respaldar lo indicado por la Jefatura de Sistemas, y con ello dar inicio a la planificación de un sistema de gestión y seguridad de información.

Con la consolidación de toda la información recolectada en este proyecto, se logró evidenciar el impacto que puede generar la no disponibilidad de los diferentes recursos y contemplar la necesidad de diseñar planes de contingencia, continuidad y de desastres que permitan garantizar y asegurar la información.

La valoración de cada uno de los hallazgos encontrados es una de los objetivos más importantes; dado que permitió identificar las causas, sus efectos y recomendaciones para la empresa.

11. RECOMENDACIONES

- El compromiso de la Alta Dirección es fundamental en el nacimiento, seguimiento e implementación del SGSI. Por lo tanto el numeral **A5. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN**, sugiere el diseño de normas, procedimientos y procesos documentados, ya que no existe una política de seguridad la cual debe ser clara, de fácil lenguaje y con un alcance definido que garantice la seguridad de la información, adicionalmente debe ser publicada y comunicada a los empleados y a las partes externas involucradas.
  Debe garantizar el diseño de objetivos y planes que permitan cumplir con el SGSI.
  Debe suministrar los recursos necesarios para el SGSI.
  Debe garantizar la realización de auditorías internas.
  Revisar periódicamente los resultados obtenidos de las auditorias.
  Comunicar permanentemente la importancia del sistema de seguridad de la información.

- En cuanto al numeral **A6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**, se recomienda que la empresa cree un comité de seguridad de la información, en el cual recae toda la responsabilidad del diseño de las políticas, la normatividad y los procedimientos.
  Elaborar y documentar todos los roles con sus respectivas responsabilidades.
  Colocar en conocimiento a la Alta Dirección, de las falencias encontradas, de tal manera que permitan la toma de decisiones y garanticen la continuidad del sistema de gestión de seguridad de la información.
  Crear un grupo interdisciplinario que involucren todas las áreas de la entidad, para que coadyuven a la sensibilización y den a conocer la importancia del sistema.
  Generar planes de comunicación, sensibilización y capacitación del SGSI.
  Diseñar controles que involucren todas las partes externas, las cuales deben garantizar la confiabilidad, integridad y disponibilidad de la información, por medio del cumplimiento de la normatividad y leyes vigentes.

- Según el numeral **A7. SEGURIDAD DE LOS RECURSOS HUMANOS** se recomienda que la empresa elabore planes que permitan realizar un seguimiento constante a los roles diseñados y del cumplimiento de las responsabilidades.
  Asegurar que las partes internas, externas se conozcan sus responsabilidades y sus roles, que minimicen la pérdida de información, de sus activos e incluso manejo inadecuado de las instalaciones de la entidad.

Debe documentar todos los acuerdos de confidencialidad con las partes externas, contemplando el inicio y la finalización de la contratación que evite divulgación de información sensible de la empresa.
Revisar periódicamente con los empleados los acuerdos que garanticen el compromiso que se adquirió en cuanto a la seguridad de la información.

- En cuanto al **A8. GESTIÓN DE ACTIVOS** se recomienda que implemente un procedimiento documentado para la gestión de los activos, que permita identificar, definir y clasificar todos los activos.
  Su equipo de seguridad debe procurar que sus activos se encuentren protegidos de tal manera que se garantice la disponibilidad, confidencialidad e integridad.
  Elaborar un inventario de activos.
  Garantizar que los activos estén asignados y delegar la debida responsabilidad para el mantenimiento de los mismos.
  Generar un plan que permita verificar el perfil idóneo que deben cumplir los empleados, contratistas, donde se establezca que cumplen con los acuerdos de confidencialidad y reserva al inicio y el término del servicio.
  Valorar la información que maneja todos sus niveles, donde garanticen los principios de la seguridad de la información.
  Generar mecanismos que garanticen la disponibilidad de los activos, que cumplan con los controles de acceso y confidencialidad apropiados.

- Según el numeral **A9 CONTROL DE ACCESO** se recomienda la implementación de un procedimiento que evalué las políticas de seguridad en cuanto al numeral de Control de Acceso, por lo anterior, se sugiere la implementación de un Directorio Activo, que asuma estas actividades y se logre minimizar al máximo los riesgos.
  Establecer, documentar y revisar la política del control de acceso, de acuerdo a las necesidades, así como los deberes y derechos que tienen los usuarios.
  Informar de los controles de acceso a todo nivel.
  Diseñar un procedimiento que establezca el control de acceso para todos los usuarios desde el inicio hasta la terminación de sus labores en la entidad.
  Diseñar un procedimiento de control de acceso para los usuarios VIP, donde se restringa el acceso a las labores propias del administrador.
  Sensibilizar a todos los miembros de la empresa, la responsabilidad que tienen con la información y las consecuencias que trae el mal uso de los sistemas.

- Según el numeral **A10. CRIPTOGRAFÍA** se sugiere contemplar la gestión y el uso de controles ya que puede permitir el uso apropiado y eficaz para proteger la confidencialidad, integridad y disponibilidad de la información.
  Gestionar para que cuente con un sistema de información o un aplicativo que permita que la información confidencial, tenga mecanismos de cifrado de datos.
  Establecer procedimientos adecuados para el manejo de la administración de claves de administradores del sistema.
  Establecer una política de cifrado que permita la trasmisión de la información reservada, y que cumpla con los principios de la seguridad.
  Establecer un proceso de seguridad, cuando se realicen las revisiones periódicas del sistema.

- Según el numeral **A11. SEGURIDAD FÍSICA Y DEL ENTORNO** se recomienda que cuente con mecanismos de seguridad como cámaras de monitoreo para el área física.
  Generar normas, que prevengan los accesos no autorizados o daños.
  Diseñar planes de contingencia física y ambiental, que aseguren la información durante la jornada laboral.
  Establecer la normatividad vigente para la seguridad física y de la información.
  Generar mecanismos que prevengan la pérdida de información, hurto o la no disponibilidad de la información.

  Lo anterior, en razón que este control, no es revisado periódicamente, y solo accede al sistema dos personas; así mismo, no se observó que el área donde se encuentra el servidor, es altamente vulnerable para cualquier acción maliciosa; se recomienda designar un lugar apropiado para el servidor, que contenga controles de humedad, temperatura y humo.

- Según el numeral **A12. SEGURIDAD DE LAS OPERACIONES** se recomienda que la empresa cuente con políticas, procedimientos y controles que permitan proteger la transferencia de la información, adicional la empresa debe implementar la protección adecuada a la información que se trasmite mediante correos electrónicos.
  Debe generar un procedimiento para el buen desarrollo de las operaciones y respuesta de incidentes.
  Debe establecer normas de seguridad para los servicios tercerizados, que garanticen la responsabilidad con la entidad.
  Debe sensibilizar al personal de la entidad, en cuanto a la importancia de software malicioso o no autorizado en los equipos
  Establecer un procedimiento que cumpla con la normatividad en cuanto al debido proceso para realizar copias de seguridad.

Generar mecanismos que protejan todos los soportes en que se encuentra la información; Discos Duros, Cd-Rom, DVD, Servidores.
Se debe proteger los servicios de comercio electrónico de las amenazas, que se puedan llevar a cabo por este medio.
Definir procedimientos que monitoreen los sistemas de información, con el fin de identificar accesos no autorizados.

- En cuanto al numeral **A13. SEGURIDAD DE LAS COMUNICACIONES** se recomienda el diseño de procedimientos documentados para estas áreas, toda vez que la parte administrativa y operativa se encuentran en el mismo sector. Se recomienda separar estas áreas y documentarlas. Las copias de respaldo se evidencian, pero esta actividad no se realiza con los procedimientos requeridos ni se encuentran salvaguardados en un área específica ni controlada.
  Generar una política de seguridad para la protección de la información en la red.
  Diseñar un procedimiento en el cual se establezcan las políticas y controles en cuanto a la transferencia de información por cualquier medio.
  Revisar periódicamente el sistema de seguridad Firewall, en donde se identifiquen las vulnerabilidades y realice el tratamiento requerido.
  Separar por grupos de trabajo los servicios de información.

- Según el numeral **A14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO SISTEMAS** establecer un procedimiento, que identifique los requerimientos de seguridad de los sistemas antes de iniciar con un desarrollo o implementación.
  Diseñar medidas de control de seguridad y registros de auditoria para los desarrollos, implementaciones y mantenimiento de los sistemas.
  Establecer un procedimiento para los cambios que se requieran a los sistemas de información, donde sean revisados y que aseguren la disponibilidad e integridad de la información.
  Elaborar un plan que permita identificar las vulnerabilidades técnicas del sistema.

- Según el numeral **A15. RELACIÓN CON LOS PROVEEDORES** se recomienda que la empresa asegure la protección de los activos de la organización que sean accesibles a los proveedores, es decir que se deben establecer medidas asociadas con el acceso a proveedores. Donde se incluya la gestión de incidentes, no se evidencio la existencia de un procedimiento que analice periódicamente estos riesgos, por lo tanto, se recomienda implementar políticas y herramientas para el cifrado de portátiles, cifrar los canales de comunicación donde transite la información sensible.

Generar una política de seguridad de la información en cuanto a la relación con los proveedores.
Diseñar los acuerdos con los proveedores, que permitan establecer los requisitos de acceso, procesamiento, almacenamiento, comunicación o suministrar información.
Todos los requisitos deben estar contemplados con la normatividad.
Definir adecuadamente los controles de inicio y finalización de los contratos.
Revisar periódicamente y auditar los servicios del proveedor.

- En cuanto al numeral **A16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN** se sugiere que la entidad elabore y coloque en marcha un plan de contingencia y continuidad, con el fin de preveer posibles fallos de los sistemas o en el supuesto de una catástrofe natural.
  Establecer mecanismos que permitan la detección y los registros de eventos informáticos.
  Elaborar políticas de incidentes de seguridad.
  Revisar periódicamente los incidentes encontrados
  Crear procedimientos específicos para los distintos incidentes que existen, tal manera que cuando sean identificados, realice en el menor tiempo posible las acciones correctivas.
  La manipulación y el acceso de los incidentes deben ser tratados por personal calificado.

- En cuanto al **A17. CONTINUIDAD NEGOCIO** debe establecer un Plan de continuidad del negocio, que permita disminuir el impacto y la recuperación por perdida de información, en el cual se identifiquen los procesos críticos para el negocio.
  Debe desarrollar procedimientos de recuperación, retorno, pruebas con el fin de asegurar la restauración de los servicios y sistemas, lo cuales deben ser revisados y actualizados periódicamente.
  De acuerdo a los riesgos identificados, el plan de contingencia debe estar orientados a los mismos.

Según el numeral **A18. CUMPLIMIENTO** se sugiere que la empresa asegure que todos los sistemas de información con los que interactúa, los cuales deben cumplir con la normatividad las políticas de la seguridad de la información, generando controles y responsabilidades. Diseñar un procedimiento que establezca los requisitos legales y contractuales. Así mismo, esta actividad debe garantizar que se realicen revisiones constantes con el fin de mejorar cada día.

Establecer mecanismos de control que garanticen la seguridad de la protección de los sistemas y las auditorias del sistema.
La información que es clasificada como confidencial se debe proteger de acuerdo al marco legal.
Los controles criptográficos establecidos deben cumplir con la normatividad vigente.

BIBLIOGRAFÍA

ANDERSON, James P. Computer Security Threat Monitoring and Surveillance. 1998. [en línea], consultado el 2 de septiembre de 2015]. Disponible en: https://www.sans.org/.../history-evolution-intrusion.

HEINEKEN TEAM. Seguridad y protección de la información: Introducción a la problemática de la seguridad informática. [en línea]. [consultado el 2 de septiembre de 2015]. Disponible en: http://www0.unsl.edu.ar/~tecno/redes%202008/seguridadinformatica.pdf agosto 2001, p.2.

ISO. Certification, ISO Survey, edición 1, Francia, 2013,2015 [en línea], [consultado el 23 de septiembre de 2015]. Disponible en: http://www.iso.org/iso/home.htm

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS. Documentación. Presentación de tesis, trabajos de grado y otros trabajos de investigación NTC 1486 sexta actualización Bogotá, 2008.

_____. Norma Técnica Colombiana, referencias bibliográficas. Contenido, forma y estructura NTC 5613, Bogotá, 2008.

_____. Norma Técnica Colombiana, referencias documentales para fuentes de información electrónicas NTC 4490,1998.

_____. Norma Técnica Colombiana, Tecnología de la información, técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos NTC-ISO-IEC 27001 primera actualización Bogotá, 2013.

_____. Norma Técnica Colombiana, Tecnología de la información, técnicas de seguridad. Código de practica para la gestión de la seguridad de la información NTC-ISO-IEC 27001 primera actualización Bogotá, 2007

NOTA ECONÓMICA. Económica empresas en ranking edición 1 [en línea] [consultado el 2 de septiembre de 2015]. Disponible en: http://www.lanotadigital.com/vademecum/small/caucho-y-plastico/plasticos-y-caucho-produccion-y-comercializacion.

PTOLOMEO.UNAM.MX. Definiciones e historia de la seguridad informática capitulo1, [en línea] [consultado el 2 de septiembre de 2015]. Disponible en:

http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/217
A4. pdf?sequence=4 Octubre de 2005, p. 7-8.

ANEXOS

DATOS DEL ENCUESTADO

Nombre:

Fecha: **Cargo:**

1. **¿Cree usted que posee información de vital importancia para la empresa?**

   SI __ NO ___

   ¿Cuáles?

2. **¿Cree usted que existen riesgos para este tipo de información. (perdida, daños, etc)?**

   SI __ NO __

   ¿Cuáles?

3. **¿Conoce las implicaciones que acarrea una posible pérdida de información o un fallo en los sistemas tecnológicos de la empresa?**

   SI ___ NO ___

   ¿Cuáles?:

4. **¿Realiza copias de seguridad o algún plan de contingencia en caso de fallos en la información o en los sistemas de información?**

   SI ___ NO ___

   ¿Con que frecuencia?:

5. **¿sabe usted de cuántos ordenadores dispone su empresa?**

   SI ___ NO ___

   ¿Cuáles?:

6. **Los ordenadores de su empresa, ¿tienen instalado antivirus?**

   SI __ NO ___

   ¿Cuáles?:

7. **¿Se realiza un mantenimiento informático periódico sobre los ordenadores de la empresa?**

   SI ___ NO ___

   ¿Cuáles?

8. **¿Disponen de servidor central de datos en su empresa?**

   SI __ NO __

   ¿Cuáles?:

9. **Sobre dicho servidor, ¿se realiza un mantenimiento informático periódico?**

   SI __ NO ___

   ¿Cuáles?:

10. **¿Dispone de baterías (SAI), APC, plantas eléctricas o algún otro dispositivo para cada ordenador y servidor, para evitar apagones o sobretensiones?**

    SI __ NO ___

    ¿Cuáles?:

11. **¿Conoce usted si la empresa tiene políticas de seguridad informática?**

    SI __ NO ___

    ¿Cuáles?

12. **¿Cuenta con un plan de contingencia en caso de un desastre natural o un mal manejo de información?**

    SI __ NO __

    ¿Cuáles?

13. **¿Conoce usted de los riesgos informáticos a los que están expuestos?**

    SI __ NO __

    ¿Cuáles?

14. **¿Siente que no está expuesto a los ataques informáticos y que su información está segura?**

    SI __ NO __

    ¿Cuáles?:

15. ¿**Usted maneja dispositivos extraíbles como: memorias usb,cd, dvd, discos duros externos?**

    SI __ NO ___

    ¿Cuáles?

16. **¿Antes de ingresar los dispositivos externos, los reporta al área de sistemas? (Responda únicamente si la anterior respuesta es afirmativa)**

    SI __ NO __

    ¿Cuáles?:

17. **¿La empresa permite el acceso a internet y redes sociales?**

    SI ___ NO ___

    ¿Cuáles?:

18. **¿Cómo manejan el ingreso al sistema informático de la empresa, por medio de usuario y claves o dispositivos electrónicos?**

    SI __ NO ___

    ¿Cuáles?:

19. **¿El acceso a los recursos de red es restringido o no?**

    SI __ NO ___

    ¿Cuáles?:

20. **¿La empresa cuenta con redes Wifi?**

    SI _X__ NO ___

21. **¿Realiza descargas de archivos desde internet (Música, videos, imágenes, etc)?**

SI ___ NO __

¿Cuáles?

PLANEACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL ÁREA DE SISTEMAS DE UNA EMPRESA FABRICANTE DE PRODUCTOS ELECTRÓNICOS BAJO LA NORMA ISO 27001:2013

Forero Lozano Natalia Ivonne
ingtataforero83@gmail.com
Bulla Valencia Katherine
katherin0911@hotmail.com
Universidad Piloto de Colombia

Abstract— This project evaluates the actual situation, based on the ISO 27001: 2013 in order to establish clearly the shortcomings that make it fails and what the possible recommendations will begin to implement the standard are, allowing be more competitive in the market. This being a value added to the main activity carried out. Also, the generation of a culture within the company, along with its consistent employees in the proper handling of information as an asset of the organization.

I. INTRODUCCIÓN

Este proyecto de grado pretende diagnosticar la situación actual de la seguridad de la información en la empresa que fábrica de productos electrónicos específicamente para el área de sistemas, inicialmente el desarrollo de este documento nace del interés de la entidad en conocer su nivel de protección en cuanto a este tema. El alcance de esta planeación de seguridad de la información está orientado para la Jefatura de Sistemas, que posee la mayoría de la información requerida para culminar con éxito este proyecto.

Tiene como principal actividad comercial la fabricación de aparatos de distribución y control de la energía electrónica; elabora, diseña, produce, y comercializa artículos electrónicos los cuales se encuentran clasificados en quince líneas, por nombrar alguna de ellas, están: la línea Doumo (maneja interruptores, pulsadores, tomacorrientes, etc.), la línea Cooper Lighting (luminarias de emergencia), línea de Tableros y Cajas Monofásicas.

II. MARCO TEORICO

A. Origen de la Seguridad.

Considerando que el ser humano desde sus orígenes ha buscado protección en todos los aspectos, como por ejemplo seguridad para la familia, seguridad en sus bienes, seguridad personal, etc., se puede considerar que este tema viene de tiempo atrás, este pensamiento fue estudiado por James P. Anderson autor del libro "Computer Security Threat Monitoring and Surveillance", el cual realizó un análisis y estableció que la seguridad nace propiamente del sentir del ser humano y ha logrado que evolucione el concepto con las necesidades propias de las personas.

La evolución del hombre y la necesidad por mejorar su calidad de vida, llegan con este proceso los sistemas informáticos que buscaron agilizar su trabajo y contener toda la información considerada para la sociedad simples datos compuestos bits y byte. Comenzó la era de los computadores y con ellos el requerimiento de conectarlos entre sí, con un propósito fundamental de enviar y recibir información; desde cualquier lugar del mundo; pero con esta falencia se generó el asegurar la información que se estaba transfiriendo. Es por esto, que se puede concluir que el hombre y los sistemas tienen un tema en un común "Protección".

Para las organizaciones y las personas en Colombia, el concepto de la seguridad de la información nace desde el momento en que se genera una necesidad de salvaguardar y proteger lo que es considerado vital y/o prioridad; todo esto se evidencia en el diario vivir y la celeridad en el que se

encuentra el mundo; estas acciones se reflejan en la urgencia por establecer protección a los procesos que coadyuvar a evitar en gran medida los riesgos que traen inherentes a ellos.

La seguridad de la información brinda desde diferentes mecanismos la identificación de amenazas y vulnerabilidades que afectan los sistemas y que generan en muchos casos daños irreparables, ocasionados por personas que poseen conocimientos en sistemas informáticos para causar daños; de esta manera se involucra a este tema: los hackers, para definir que es, el diccionario Merrian-Webster establece una definición "una persona que secretamente tiene acceso a un sistema informático con el fin de obtener información, causa daños, etc.: una persona que interviene negativamente en un sistema informático".

B. Políticas de Seguridad

Teniendo en cuenta que la empresa busca conocer el estado actual de su seguridad mediante un diagnóstico de seguridad de la información; y un punto importante para dar inicio a la implementación de un sistema de seguridad, son las políticas de seguridad. Estas políticas no son netamente un mecanismo de sanción, es un concepto de saber que se quiere proteger y cómo hacerlo. Contemplar una política y que haya éxito, corresponde hacer parte a todo el personal de la entidad y de reconocer la información como activo. Por tal razón se deben establecer unos requisitos que se deben establecer para el personal que intervienen directa e indirectamente a los sistemas de información y deben ser de tipo:

- Prohibitiva, es decir, todo lo que no está expresamente permitido está denegado.
- Permisiva, es decir, todo lo que no está expresamente prohibido está permitido.

C. Responsables.

La política de seguridad contempla la necesidad de delegar responsabilidades; es decir, personal encargado de hacer que estas políticas sean cumplidas en la empresa, cuenta con un Ingeniero de Sistemas para toda la planta, y no posee el apoyo requerido por parte de la Alta Dirección para que las políticas se lleven a cabo. Se debe contar con personal especialista en seguridad informática que cumpla las funciones de supervisión, cumplimiento, mantenimiento, actualizaciones, capacitaciones e informes periódicamente a gerencia. Para la realización de estas políticas se deben tener en cuenta la normatividad que coadyuvan a la empresa a poseer una mejor gestión de seguridad informática.

D. *Norma ISO 27001:2013*

Es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. Además esta norma establece 114 controles que permiten a la organización cumplir con los requisitos de seguridad de la propia organización estableciendo los tres principios fundamentales en los que se basa la seguridad informática que son:

1) Confiabilidad de los datos: se refiere a la capacidad del sistema para evitar que personas o procesos no autorizados puedan acceder a la información almacenada en él.

2) Disponibilidad de los datos: se refiere a él funcionamiento eficientemente y que es capaz de recuperarse rápidamente en caso de falla. Es decir que la información se pueda utilizar cuando se requiera.

3) Integridad de los datos: el sistema no debe modificar ni corromper la información que almacena, o permitir que alguien no autorizado lo haga. Permitiendo asegurar que no ha sido falsificada la información. Teniendo en cuenta que este tipo de norma puede ser implementada en cualquier tipo de organización ya sea grande, pequeña, privada o pública. Es por este motivo es seleccionada la empresa fabricante de productos electrónicos para la realización de una propuesta de gestión y seguridad basado en la norma ISO 27001:2013.

E. ¿Por qué es necesaria la seguridad de la información en la empresa que fábrica de productos electrónicos?

Es necesaria la seguridad de la información toda vez que esta empresa actualmente no cuenta con políticas de seguridad que brinden protección a los sistemas de información. La inexistencia de las políticas constantemente está expuesta a fraudes, daños y/o ataques.

Esto puede conllevar a causar varios daños en cuanto a su competitividad, rentabilidad, el cumplimiento legal y la imagen empresarial.

F. Ciclo PHVA (Planificar, hacer, verificar y actuar)

Este modelo es utilizado para realizar la implementación de un sistema de gestión de seguridad informática dado que permite realizar las actividades que marquen un orden lógico, organizado y que permita lograr un buen diagnóstico para *esta entidad,* por lo tanto, este proyecto se basa en la etapa de planificar.

1) Planificar

Definir políticas de seguridad.
Determinar el alcance.
Valorar activos.
Analizar el riesgo.
Gestionar el riesgo.
Aplicar controles de la norma ISO 27001.

2) Hacer

Implementar plan de gestión de riesgos, Código de práctica para la gestión de la seguridad de la información.
Implementar controles.

3) Verificar

Verificación de implementación de gestión de riesgo.
Revisión de procesos de monitoreo.
Revisión de niveles de riesgo.
Revisión de auditorías internas.

4) Actuar

Implementaciones de mejoras.
Adoptar medidas preventivas y correctivas.
Comunicación de resultados.

III. METODOLOGÍA

A. Diseño

Se realizó un diagnóstico, bajo el concepto completamente académico, que permitió evidenciar los riesgos de la entidad, aplicando dos instrumentos para verificar la información (encuestas) al área de sistemas y (cuestionarios) para los usuarios que acceden al sistema.

Así mismo, se utilizó una matriz de riesgo para el proceso en estudio (Jefatura de Sistemas) que permitió organizar cada uno de los dominios, objetivos de control, riesgos y controles establecidos en el Anexo A de la norma ISO 27001: 2013, de tal manera que el resultado de este instrumento permita mitigar los riesgos más importantes como también obtener una visión más clara de la situación real de esta área.

Los datos que hicieron parte de esta matriz, fueron considerados como información de alta confiabilidad, dado que se extrajeron directamente por parte del Jefe de la Jefatura de Sistemas y por el personal que hace parte de la empresa que fabrica productos electrónicos.

B. Participantes

Las personas que participaron en esta propuesta son una muestra de los empleados y usuarios que manipulan y/o accede de los sistemas de información que maneja la entidad. Los empleados que participaron son profesionales, directamente encargados de los sistemas de información y seguridad. Por su parte los usuarios, fueron personas vinculadas a la empresa fabricante de productos electrónicos que utilizan los recursos informáticos, más no directamente relacionados con el área de seguridad.

La entidad cuenta con una persona vinculada al área de seguridad, que participó en el estudio. Así mismo, se consideraron cuarenta (40) usuarios de los sistemas de información, de los cuales se seleccionó una muestra aleatoria representativa equivalente al 75% de la población.

C. Instrumentos

Se diseñó una encuesta (para aplicación virtual o en papel) de 133 ítems (preguntas cerradas, para que el personal vinculado al área de seguridad que evalué el sistema, bajo unos estándares previamente establecidos **(Ver anexo 2).** De igual forma, se creó un breve cuestionario con 21 ítems (preguntas abiertas).

IV. RESULTADOS

A. Encuesta

Se aplica el instrumento de la encuesta a los usuarios que acceden al sistema, con la finalidad de identificar y verificar cual es la percepción que tiene el usuario final sobre la seguridad de la información que maneja la entidad, para esto se diseñaron 21 preguntas que permitieran observar la realidad; en donde 1 representa SI y 2 representa NO.

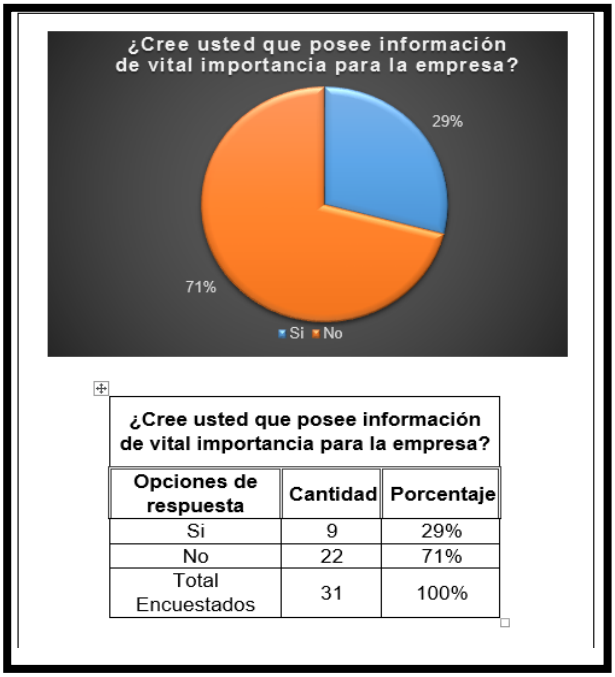
A continuación, algunas de las preguntas que se aplicaron:

CUADRO I
Consolidado Resultados Aplicación de Cuestionario Diagnóstico de Seguridad de la Información para la empresa que fabrica productos electrónicos

Número de encuestas	¿Cree usted que posee información de vital importancia para la empresa?	¿Cree usted que existen riesgos para este tipo de información. (Perdida, daños, etc)?
1	1	2
2	1	1
3	1	2
4	1	2
5	1	2
6	1	1
7	2	1
8	2	2
9	2	2
10	2	2
11	2	1
12	1	2
13	1	2
14	1	1
15	2	2
16	2	1
17	2	2
18	2	2
19	2	2
20	2	1
21	2	2
22	2	1
23	2	2
24	2	1
25	2	1
26	2	1
27	2	2
28	2	2
29	2	2

30	2	2
31	2	2

Figura 1. Resultado estadístico pregunta No. 1



¿Cree usted que posee información de vital importancia para la empresa?		
Opciones de respuesta	**Cantidad**	**Porcentaje**
Si	9	29%
No	22	71%
Total Encuestados	31	100%

Fuente: Autores

Teniendo en cuenta con la Figura 2. se puede observar que el 71% de los encuestados desconocen si poseen información sensible de la entidad; esto permite indicar que el numeral A.7 (Seguridad de los Recursos Humanos) del anexo A de la norma ISO 27001:2013 se esta incumpliendo.

B. Matriz de Riesgos y Acciones Mitigantes

Durante el proceso de recolección de información, y como mecanismo para hallar los riesgos de la empresa, se realizó una matriz de riesgos y las acciones mitigantes, que permitió documentar los numerales que están siendo incumplidos y/o cumplidos; luego ubicar la información en Zonas de Riesgos, para facilitar su consulta.

1) Valoración del riesgo

CUADRO II
Valores de riesgo

Probabilidad	Valor	Zonas de Riesgo		
3	Alta	15 Moderado	30 Importante	60 Inaceptable
2	Media	10 Tolerable	20 Moderado	40 Importante
1	Baja	5 Aceptable	10 Tolerable	20 Moderado
	Impacto	Leve	Moderada	Catastrófica
	Valor	5	10	20

Fuente: Autores

En esta parte del proyecto, el proceso de identificación de los riesgos en la empresa que fábrica de productos electrónicos, se contempló manejar el *Cuadro II Valores del riesgo.* El uso de este cuadro permitió establecer en qué estado se encuentra en la entidad bajo la norma ISO 27001:2013. Consiste en la verificación de la probabilidad en que ocurra el evento Vs el impacto de ocurrencia del evento y la criticidad del riesgo.

Cada una de las zonas de riesgo tiene un tratamiento especial para los riesgos encontrados:

Inaceptable: corresponde al nivel de riesgo más alto y el cual contempla que los riesgos encontrados deben ser controlados de manera inmediata, capaz de prevenir, reducir, transferir o compartir el riesgo.

Importante: corresponde a un nivel de riesgo más alto y el cual contempla que los riesgos encontrados deben ser controlados de manera inmediata, capaz de prevenir, reducir, transferir o compartir el riesgo.

Moderado: deben ser tratados con un fin, evitarlos.

Tolerable: corresponde a un nivel permisible, de tal manera que se deben monitorear para que se reduzcan eficientemente.

Aceptable: corresponde a nivel en el cual se deben monitorear para que los riesgos no pasen a un nivel de criticidad superior.

2) Matriz de Riesgos

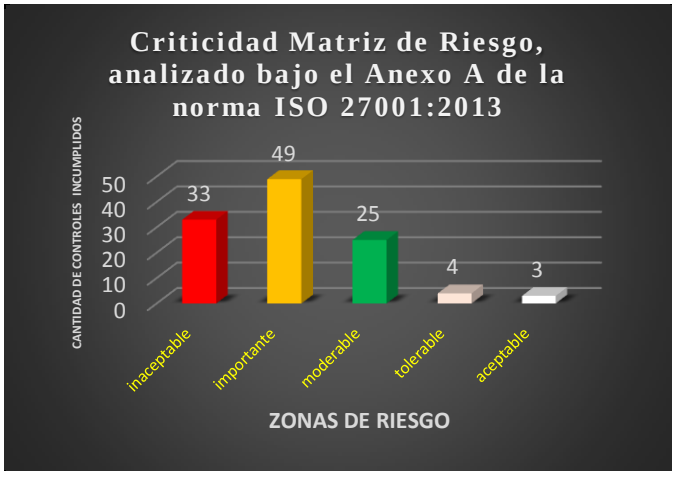
TABLA I
Matriz de Riesgos

Vulnerabilidad	Descripción vulnerabilidad	Consecuencia	Control	Responsable	Ejecutante	Prob vs imp.
Políticas de seguridad	Desconocimiento de la importancia de la seguridad de la información	Desasegura miento de la información	Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y partes interesadas	Alta dirección - Área de sistemas	Área de sistemas	60
Seguridad en Recursos Humanos	Falta de establecer roles y responsabilidades	Mal manejo de la información por el personal	Se deben definir y asignar todas las responsabilidades de la seguridad de la información	Área de sistemas	Área de sistemas	20

Fuente: Autores.

Esta matriz evidencia alguno de los dominios que tienen criticidad y la cantidad de controles incumplidos por la empresa que fabrica productos electrónicos, este análisis es basado en el Anexo A de la norma ISO 27001:2013; el resultado del instrumento de la encuestas realizadas, confirman la información obtenida de este planeamiento.

Figura 2. Criticidad Matriz de Riesgo - Objetivos de Control



Fuente: Autores.

De acuerdo con la Figura 23, refleja la criticidad de las zonas de riesgo establecidas bajo la matriz de riesgo y la cantidad de controles incumplidos por la empresa que fábrica de productos electrónicos. En cuanto al análisis del Anexo A de la norma ISO 27001:2013; el resultado del instrumento de la encuestas realizadas, confirman la información obtenida de este planeamiento.

V. VERIFICACIÓN Y APLICACIÓN DE LA NORMA ISO 27001 PARA LA EMPRESA QUE FÁBRICA PRODUCTOS ELECTRÓNICOS

Con el fin de realizar una propuesta adecuada para esta entidad, se realizó inicialmente una visita de campo en sitio, que permitiera reflejar las falencias que tiene actualmente en seguridad de la información. Teniendo en cuenta lo anterior, se da inició a la evaluación de los numerales de la norma y subitem de la ISO 27001:2013. Así mismo, y con el propósito de mantener un orden de los hallazgos encontrados por numeral, se designó un número consecutivo para lograr una mejor coherencia en los resultados.

A. Hallazgo 01 Política para la Seguridad de la Información

Fecha: 03 de agosto de 2015.
Numeral: Políticas para la seguridad de la información.

Subitem:
Orientación de la dirección para la Gestión de la Seguridad de la Información.
Revisión de las Políticas para seguridad de la información. Las Políticas para Seguridad de la Información se deben revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su idoneidad, adecuación y eficacia continúas.

Criterio: Verificar si en la empresa que fábrica de productos electrónicos se encuentran implementadas Políticas de Seguridad, las cuales deberán estar aprobadas, hayan sido publicadas y difundidas para todo el personal.

Causa: Desconocimiento de la importancia de la seguridad de la información en la entidad.

Efecto:

Información no segura.
Incumplimiento a los parámetros establecidos internos y externos que el sistema proporciona.
Falta de control del sistema de información de la empresa.

Conclusión: la empresa que fabrica productos electrónicos no cumple con la política de seguridad establecida en la norma ISO 27001; lo que indica en primera medida el desconocimiento de la Alta Gerencia de la importancia que tiene la seguridad de la información en la entidad.

Recomendación: Orientar la construcción de la política de seguridad en la empresa, clara, y con unos objetivos que permitan asegurar la continuidad del negocio.

El área de sistemas debe propender por colocar en conocimiento de las ventajas y desventajas de implementar un sistema de seguridad de la información en la entidad.

B. Hallazgo 02 Organización de la Seguridad de la Información.

Fecha: 03 de agosto de 2015.
Numeral: Organización de la Seguridad de la Información.

Subitem:
Organización Interna.
Dispositivos Móviles y Teletrabajo.

Criterio: Verificar la existencia si en la empresa que fabrica productos electrónicos, existen políticas de seguridad adecuadas para el manejo de la organización interna y dispositivos móviles y teletrabajo.

Causa:

- No se encuentran definidos ni documentados los roles y responsabilidades del personal.
- No se evidencia contacto con autoridades pertinentes.
- Se evidencian la existencia de mínimas políticas de seguridad en cuanto al acceso de dispositivos móviles.
- No se evidencia una política que contenga medidas de seguridad para salvaguardar la información, la cual es manipulada por todo el personal administrativo y operativo.
- Se evidencia que se realizan actividades propias del área de sistemas en áreas ajenas a ella, pero no se encuentran documentadas ni registradas.

Efecto:

- Negligencia por parte del personal, el cual puede ser calculado en pérdidas.
- Pérdida de información.
- Desconocimiento de temas asociados al tema de seguridad-no existe un medio para retroalimentar fallos del sistema por el personal.

Conclusión: No se evidencia el establecimiento de políticas de seguridad para la organización interna ni para el uso de dispositivos móviles y teletrabajo

Recomendación: Se sugiere establecer políticas de seguridad para el personal que interviene en el sistema, que garanticen la corresponsabilidad del personal y las Directivas, así como las restricciones pertinentes para los dispositivos móviles.

VI. CONCLUSIÓN

Este análisis de seguridad para la empresa que fabrica productos electrónicos, permitió realizar una planificación de un sistema de gestión y seguridad de la información para el área de sistemas bajo la norma ISO 27001:2013.

Frente al cumplimiento de la norma, el Sistema de Seguridad se encuentra en la primera etapa de madurez, y los resultados que se evidenciaron en este trabajo, reflejan la situación actual por la falta de un seguimiento periódico.

Al elaborar el análisis de riesgo para la empresa que fabrica productos electrónicos, basado en la norma ISO ISO27001:2013 y 27001:2015, permitió identificar con mayor claridad las falencias que se encuentran en todos los niveles de la entidad, y que requieren ser tratados en el menor tiempo posible.

Podemos establecer que la entidad, no cuenta con un mecanismo de comunicación eficiente, que permita divulgar oportunamente los objetivos, políticas de seguridad de la información y las expectativas que se tiene en cuanto a la planificación de un sistema de gestión de información basado en la norma ISO27001:2013 y 27001:2015.

De acuerdo a las encuestas y entrevistas realizadas en la empresa se obtuvo información de gran interés que permitió respaldar lo indicado por la Jefatura de Sistemas, y con ello dar inicio a la planificación de un sistema de gestión y seguridad de información.

Con la consolidación de toda la información recolectada en este proyecto, se logró evidenciar el impacto que puede generar en la empresa que fabrica productos electrónicos la no disponibilidad de los diferentes recursos y contemplar la necesidad de diseñar planes de contingencia, continuidad y de desastres que permitan garantizar y asegurar la información.

La valoración de cada uno de los hallazgos encontrados es una de los objetivos más importantes; dado que permitió identificar las causas, sus efectos y recomendaciones para la empresa.

VII. RECOMENDACIONES

El compromiso de la Alta Dirección de la entidad, es fundamental en el nacimiento, seguimiento e implementación del SGSI. Por lo tanto el numeral A5. Políticas de Seguridad de la Información, sugiere el diseño de normas, procedimientos y procesos documentados, ya que no existe una política de seguridad la cual debe ser clara, de fácil lenguaje y con un alcance definido que garantice la seguridad de la información, adicionalmente debe ser publicada y comunicada a los empleados y a las partes externas involucradas. Debe garantizar el diseño de objetivos y planes que permitan cumplir con el SGSI. Debe suministrar los recursos necesarios para el SGSI. Debe garantizar la realización de auditorías internas. Revisar periódicamente los resultados obtenidos de las auditorias. Comunicar permanentemente la importancia del sistema de seguridad de la información.

En cuanto al numeral A6. Organización de la Seguridad de la Información, se recomienda que crear un comité de

seguridad de la información, en el cual recae toda la responsabilidad del diseño de las políticas, la normatividad y los procedimientos. Elaborar y documentar todos los roles con sus respectivas responsabilidades. Colocar en conocimiento a la Alta Dirección, de las falencias encontradas, de tal manera que se tomen decisiones y garanticen la continuidad del sistema de gestión de seguridad de la información. Crear un grupo interdisciplinario que involucren todas las áreas de la entidad, para que coadyuven a la sensibilización y den a conocer la importancia del sistema. Generar planes de comunicación, sensibilización y capacitación del SGSI. Diseñar controles que involucren todas las partes externas, las cuales deben garantizar la confiabilidad, integridad y disponibilidad de la información, por medio del cumplimiento de la normatividad y leyes vigentes.

Según el numeral A7. Seguridad de los Recursos Humanos se recomienda que la empresa elabore planes que permitan realizar un seguimiento constante a los roles diseñados y del cumplimiento de las responsabilidades. Asegurar que las partes internas, externas de la entidad conozcan sus responsabilidades y sus roles, que minimicen la pérdida de información, de sus activos e incluso manejo inadecuado de las instalaciones de la entidad. Debe documentar todos los acuerdos de confidencialidad con las partes externas, contemplando el inicio y la finalización de la contratación que evite divulgación de información sensible de la empresa. Revisar periódicamente con los empleados los acuerdos que garanticen el compromiso que se adquirió en cuanto a la seguridad de la información.

En cuanto al A8. Gestión de Activos se recomienda que la empresa implemente un procedimiento documentado para la gestión de los activos, que permita identificar, definir y clasificar todos los activos. Su equipo de seguridad debe procurar que sus activos se encuentren protegidos de tal manera que se garantice la disponibilidad, confidencialidad e integridad. Elaborar un inventario de activos. Garantizar que los activos estén asignados y delegar la debida responsabilidad para el mantenimiento de los mismos. Generar un plan que permita verificar el perfil idóneo que deben cumplir los empleados, contratistas, donde se establezca que cumplen con los acuerdos de confidencialidad y reserva al inicio y el término del servicio. Valorar la información que maneja en todos sus niveles, donde garanticen los principios de la seguridad de la información. Generar mecanismos que garanticen la disponibilidad de los activos, que cumplan con los controles de acceso y confidencialidad apropiados.

Según el numeral A9 Control de Acceso se recomienda que la entidad implemente un procedimiento que evalué las políticas de seguridad en cuanto al numeral de Control de Acceso, por lo anterior, se sugiere la implementación de un Directorio Activo, que asuma estas actividades y se logre minimizar al máximo los riesgos. Establecer, documentar y revisar la política del control de acceso, de acuerdo a las necesidades del negocio, así como los deberes y derechos que tienen los usuarios. Informar de los controles de acceso a todo nivel. Diseñar un procedimiento que establezca el control de acceso para todos los usuarios desde el inicio hasta la terminación de sus labores en la entidad. Diseñar un procedimiento de control de acceso para los usuarios VIP, donde se restringa el acceso a las labores propias del administrador. Sensibilizar a todos los miembros de la empresa, la responsabilidad que tienen con la información y las consecuencias que trae el mal uso de los sistemas.

Según el numeral A10. Criptografía se sugiere contemplar la gestión y el uso de controles ya que puede permitir el uso apropiado y eficaz para proteger la confidencialidad, integridad y disponibilidad de la información. Gestionar para que la empresa cuente con un sistema de información o un aplicativo que permita que la información confidencial, tenga mecanismos de cifrado de datos. Establecer procedimientos adecuados para el manejo de la administración de claves de administradores del sistema. Establecer una política de cifrado que permita la trasmisión de la información reservada, y que cumpla con los principios de la seguridad. Establecer un proceso de seguridad, cuando se realicen las revisiones periódicas del sistema.

Según el numeral A11. Seguridad Física y del Entorno se recomienda que la empresa, cuente con mecanismos de seguridad como cámaras de monitoreo para el área física. Generar normas, que prevengan los accesos no autorizados o daños en las instalaciones como en los activos. Diseñar planes de contingencia física y ambiental, que aseguren la información durante la jornada laboral. Establecer la normatividad vigente para la seguridad física y de la información. Generar mecanismos que prevengan la pérdida de información, hurto o la no disponibilidad de la información. Lo anterior, en razón que este control, no es revisado periódicamente, y solo accede al sistema dos personas; así mismo, no se observó que el área donde se encuentra el servidor, es altamente vulnerable para cualquier acción maliciosa; se recomienda designar un lugar apropiado para el servidor, que contenga controles de humedad, temperatura y humo.

Según el numeral A12. Seguridad de las Operaciones se recomienda que la empresa cuente con políticas, procedimientos y controles que permitan proteger la transferencia de la información, adicional la empresa debe implementar la protección adecuada a la información que se trasmite mediante correos electrónicos. Debe generar un procedimiento para el buen desarrollo de las operaciones y respuesta de incidentes. Debe establecer normas de seguridad para los servicios tercerizados, que garanticen la responsabilidad con la entidad. Debe sensibilizar al personal de la entidad, en cuanto a la importancia de software malicioso o no autorizado en los equipos de Ave Colombiana S.A.S. Establecer un procedimiento que cumpla con la normatividad en cuanto al debido proceso para realizar copias de seguridad. Generar mecanismos que protejan todos los soportes en que se encuentra la información; Discos Duros, Cd-Rom, DVD, Servidores. Se debe proteger los servicios de comercio electrónico de las amenazas, que se puedan llevar a cabo por este medio. Definir procedimientos que monitoreen los

sistemas de información de la entidad, con el fin de identificar accesos no autorizados.

En cuanto al numeral A13. Seguridad de las Comunicaciones se recomienda el diseño de procedimientos documentados para estas áreas, toda vez que la parte administrativa y operativa se encuentran en el mismo sector. Se recomienda separar estas áreas y documentarlas. Las copias de respaldo se evidencian, pero esta actividad no se realiza con los procedimientos requeridos ni se encuentran salvaguardados en un área específica ni controlada. Generar una política de seguridad para la protección de la información en la red. Diseñar un procedimiento en el cual se establezcan las políticas y controles en cuanto a la transferencia de información por cualquier medio. Revisar periódicamente el sistema de seguridad Firewall, en donde se identifiquen las vulnerabilidades y realice el tratamiento requerido. Separar por grupos de trabajo los servicios de información de la entidad.

Según el numeral A14. Adquisición, Desarrollo y Mantenimiento Sistemas establecer un procedimiento, que identifique los requerimientos de seguridad de los sistemas de la empresa, antes de iniciar con un desarrollo o implementación. Diseñar medidas de control de seguridad y registros de auditoria para los desarrollos, implementaciones y mantenimiento de los sistemas. Establecer un procedimiento para los cambios que se requieran a los sistemas de información, donde sean revisados y que aseguren la disponibilidad e integridad de la información. Elaborar un plan que permita identificar las vulnerabilidades técnicas del sistema.

Según el numeral A15. Relación con los Proveedores se recomienda que la empresa asegure la protección de los activos de la organización que sean accesibles a los proveedores, es decir que se deben establecer medidas asociadas con el acceso a proveedores. Donde se incluya la gestión de incidentes, no se evidencio la existencia de un procedimiento que analice periódicamente estos riesgos, por lo tanto, se recomienda implementar políticas y herramientas para el cifrado de portátiles, cifrar los canales de comunicación donde transite la información sensible. Generar una política de seguridad de la información en cuanto a la relación con los proveedores. Diseñar los acuerdos con los proveedores, que permitan establecer los requisitos de acceso, procesamiento, almacenamiento, comunicación o suministrar información de la entidad Todos los requisitos deben estar contemplados con la normatividad. Definir adecuadamente los controles de inicio y finalización de los contratos. Revisar periódicamente y auditar los servicios del proveedor.

En cuanto al numeral A16. Gestión de Incidentes de Seguridad de la Información se sugiere que la entidad elabore y coloque en marcha un plan de contingencia y continuidad, con el fin de prever posibles fallos de los sistemas o en el supuesto de una catástrofe natural. Establecer mecanismos que permitan la detección y los registros de eventos informáticos. Elaborar políticas de incidentes de seguridad. Revisar periódicamente los incidentes encontrados en la empresa. Crear procedimientos específicos para los distintos incidentes que existen, tal manera que cuando sean identificados, realice en el menor tiempo posible las acciones correctivas. La manipulación y el acceso de los incidentes deben ser tratados por personal calificado.

En cuanto al A17. Continuidad Negocio debe establecer un Plan de continuidad del negocio, que permita disminuir el impacto y la recuperación por perdida de información, en el cual se identifiquen los procesos críticos para el negocio. Debe desarrollar procedimientos de recuperación, retorno, pruebas con el fin de asegurar la restauración de los servicios y sistemas de la empresa, lo cuales deben ser revisados y actualizados periódicamente. De acuerdo a los riesgos identificados, el plan de contingencia debe estar orientados a los mismos.

Según el numeral A18. Cumplimiento se sugiere que la empresa asegure que todos los sistemas de información con los que interactúa, los cuales deben cumplir con la normatividad las políticas de la seguridad de la información, generando controles y responsabilidades. Diseñar un procedimiento que establezca los requisitos legales y contractuales. Así mismo, esta actividad debe garantizar que se realicen revisiones constantes con el fin de mejorar cada día. Establecer mecanismos de control que garanticen la seguridad de la protección de los sistemas y las auditorias del sistema. La información que es clasificada como confidencial de la entidad se debe proteger de acuerdo al marco legal. Los controles criptográficos establecidos deben cumplir con la normatividad vigente.

REFERENCIAS

[1] Instituto Colombiano de Normas Técnicas. Documentación. Presentación de tesis, trabajos de grado y otros trabajos de investigación NTC 1486 sexta actualización Bogotá, 2008.

[2] Norma Técnica Colombiana, referencias bibliográficas. Contenido, forma y estructura NTC 5613, Bogotá, 2008.

[3] Norma Técnica Colombiana, referencias documentales para fuentes de información electrónicas NTC 4490,1998.

[4] Norma Técnica Colombiana, Tecnología de la información, técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos NTC-ISO-IEC 27001 primera actualización Bogotá, 2013.
Norma Técnica Colombiana, Tecnología de la información, técnicas de seguridad. Código de practica para la gestión de la seguridad de la información NTC-ISO-IEC 27001 primera actualización Bogotá, 2007.

[5] A, James P. (1998) Computer Security Threat Monitoring and Surveillance. Disponible en: https://www.sans.org/.../history-evolution-intrusion.

[6] H. TEAM. (2001) Seguridad y Protección de la información: Introducción a la problemática de la seguridad informática. Disponible en:http://www0.unsl.edu.ar/~tecno/redes%202008/seguridadinformatica.pdf agosto 2001, p.2.
PTOLOMEO.UNAM.MX. (2005). Definiciones e historia de la seguridad informática capitulo1. Disponible en: http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/217 A4. pdf?sequence=4 Octubre de 2005, p. 7-8.